HISTORY OF AMERICAN SURVEILLANCE & THE SNOWDEN FILES: VIOLATIONS OF THE FOURTH AMENDMENT'S PRIVACY RIGHTS

MARY "LIBBY" ENNIS & ASNA NAYANI
College of Engineering & College of Arts and Letters
Florida Atlantic University

Abstract

Surveillance has been a longstanding tradition in the United States, dating back to even the colonial period. The full scope of American surveillance programs has only expanded since then, growing unregulated and encroaching on what should be protected by the country's Constitution. This came to a head in 2013, when Edward Snowden published a variety of files that exposed the U.S. government--the National Security Agency (NSA) in particular--for its violations of privacy, cybersecurity, and human rights. While Snowden was charged with offenses against the Espionage Act of 1917, he managed to escape to and currently resides in Russia. His files revealed the U.S. government's extensive surveillance of American citizens in collaboration with multiple international governments and organizations. This clear transgression of internet privacy fundamentally changes the relationship between governments and their citizens, the latter being monitored without their consent or knowledge and the former hiding behind fragile justifications. The authority and access to information governments hold regarding their own citizens should be public knowledge and open to public scrutiny.

History of U.S. Surveillance

In our contemporary digital world, surveillance surrounds us in countless ways, whether it is through the government, tech companies, or even the people around us. Whether people are aware of it or not, surveillance has become embedded in our everyday lives. While many would trace this back to the 20th century, surveillance has always been within American culture, as far back as the Colonial era. The National Research Council

defines the term as the following, "'Surveillance' may be thought of as systematic attention to personal details for the purposes of influence, management, or control…"[1] With technological advancements and new threats "...the intensity and scope of surveillance have varied since the 17th century, [but] the same factors shape them: the interests of those in positions of power, the technology available to them, and the legal frameworks within which they operate." [2] The legality surrounding surveillance is constantly debated, especially when services for public good can very quickly morph into tools for monitoring citizens. Contemporary surveillance has continuously grown in scope and has now become a clear invasion of privacy.

Surveillance has always been a part of American culture, whether it was recognized as such or not. During the Colonial period, surveillance was mutually shaped by the Puritan faith and government.[3] Neighbors watched each other to ensure a moral standard set by Puritanism was met, if not the government could intervene for potential crimes.[4] Despite Puritans' aversion to government, considering their prosecution in England, the relationship between faith and government was incredibly close and mutually reinforced.[5] However, this relationship had its limits due to established legal codes, "As early as 1647, Rhode Island adopted the principle that 'a man's house is his castle,'...The colony outlawed 'forcible Entry and Detainer' into a private dwelling, except by law enforcement officers acting under exceptional circumstances."[6] While surveillance was a local effort during this time, the government from a very young age established that a right to privacy was owed to its citizens. The protection of someone's private property, with the exception of

[1] James Waldo, Herbert Lin & Lynette I. Millett, *A Short History of Surveillance and Privacy in the United States, in Engaging Privacy and Information Technology in a Digital Age* 349 (2007).
[2] *Id.*
[3] I*d.*
[4] *Id.*
[5] *Id.*
[6] *Id.*

probable cause, was a foundational right that existed even prior to the formation of the American government.

The beginning of America, during the late 18th and early 19th century, saw a shift in surveillance. "The origins of institutional surveillance in Western society can be generally traced back to the establishment of the modern bureaucracy, which had its beginnings in the military organization, the bureaucratic state, and the capitalist enterprise."[7] The early skirmishes that would lead to the revolutionary war forced the creation of a central army.[8] In doing so, the once divided militia became a central force that could identify its soldiers and maintain records for the sake of order.[9] The establishment of the Continental Congress, and later the central US government, after the Revolutionary war, became the center of surveillance with the goal of record-keeping.[10] The primary method of surveillance at this time was the national census; it was the first universal survey of citizens, originally implemented in 1790 to keep track of voters in the new democracy.[11] In its early years, the census only collected very "basic data on the gender, color, and identity of free males above the age of 16 years."[12] Commerce also played a role in surveillance due to business becoming more bureaucratic and collecting records, some of which were able to directly identify individuals.[13] The era of the revolutionary war was the first time surveillance was used as a political tool to check loyalties.[14] While the American Revolution was being fought against England, the Patriots and Loyalists were facing a domestic battle; suspicion of Loyalists became constant, especially when it was unknown if they were close to you, and surveillance became a means to

[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] *Id.*
[14] *Id.*

identify them.[15] While there was certainly a rise in surveillance since the Colonial era, the establishment of the U.S. government and the Constitution guaranteed basic rights to citizens that prevented the government from overstepping.[16] This balanced out the surveillance occurring because the record-keeping was limited, and arguably necessary, and after the Revolutionary War, suspicions of individuals died down since a clear winner was established.

The period between the Civil War and the mid-20th century fundamentally changed the accessibility and scope of surveillance as vast technological advancements made information collection significantly easier. "The balance of surveillance and individual rights was upset by unprecedented technological development, the rapid growth of bureaucratic institutions (both governmental and commercial), and the failure of lawmakers to formulate adequate legal protections against surveillance practices."[17] The development of the telegraph, fingerprint collection, camera, and other technology made it possible to track information more accurately than ever, especially when these technologies were adopted by the government.[18] In the beginning, this information mainly remained on a local level. But it quickly expanded to a national level with the expansion of the census both as a bureaucratic organization with the creation of the Census Office and as it began to ask more personal questions.[19] These activities grew further in scope and legality due to loyalty testing during the Civil War, World War I, and World War II with the Espionage Act being passed in 1917.[20] Government agencies such as the IRS and Social Security Administration were able to gain access to personal information in order to collect income tax or distribute New Deal benefits respectively.[21] However,

[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] I*d.*
[19] *Id.*
[20] *Id.*
[21] *Id.*

"This uneasy combination of social benefits and regulatory mechanisms would come to define the nature of bureaucratic surveillance in the 20th century, as it continually oscillated between the provision of care and the exercise of control."[22]

As surveillance increased, both through government records and individual uses of new technologies, the law could not keep up and private property protection was not enough to cover the scope of monitoring occurring now. While the Telecommunications Act of 1934 did prevent the government from using intercepted communication as legal evidence in court, they still continued to collect such information for other uses.[23] This lack of regulation that simultaneously occurred with mass technological development made it so that the U.S. government could now gain mass information on their citizens, especially during uncertain times such as war.

The Cold War was an era of distrust with rampant fear of Communist spies overtaking the nation. To combat this, the U.S. utilized their surveillance technology, alongside the newly developed computers, to test citizens' loyalty.[24] However, the scope of this surveillance grew beyond foreign spies and quickly became used in what the government identified as domestic threats. "In the 1950s, the enemies were Communists; in the 1960s, black rights activists; and in the late 1960s and early 1970s, antiwar protesters. The existence of these groups was believed to justify the federal government's development of security records to monitor anyone deemed a threat."[25] This was no longer about simply monitoring foreign threats, it was now about monitoring what the government deemed to be deviant, even when what these groups were doing was perfectly legal.

---

[22] *Id.*
[23] *Id*
[24] *Id.*
[25] *Id.*

Surveillance would come to the forefront of public attention in 1972 with the Watergate scandal which forced the government to pass the Privacy Act of 1974.[26] The scope of the act would be limited. Despite the fact that the first draft demanded federal, state, local, and private regulation of surveillance, in the end, the bill encompassed only the federal government and private businesses it consulted. [27] Indeed, this repeal of what the law intended to achieve with enforcement measures could have made enforcement of such laws significantly more difficult and able to erode more easily. Most recently, when the Supreme Court in the *Dobbs, State Health Officer Of The Mississippi Department Of Health, Et Al. v. Jackson Women's Health Organization Et Al*.[28] chose to overturn the 1973 decision of *Roe v. Wade*,[29] a decision based on the right to privacy, once again the court chose to deregulate and diminish the right to privacy.

Surveillance has always been a part of the American experience, but the extent to which it has grown, especially in times of crisis, is incredibly alarming. Once a decentralized process that could be avoided, it has now become inescapable in the modern, digital world. While surveillance programs prior to the 21st century were already invasive, they have only continued to grow.

9/11 and The P.A.T.R.I.O.T Act

On September 11, 2001, terrorists from the group al-Qaeda crashed three planes into the Twin Towers of the World Trade Center and Pentagon

[26] *Id.*
[27] *Id.*
[28] Dobbs, State Health Officer Of The Mississippi Department Of Health, Et Al. v. Jackson Women's Health Organization Et Al., No 19-1392, slip op. at 1 (cert. granted to the U.S. Ct. of Appeals, 5th Cir.), (June 24, 2022), https://supreme.justia.com/cases/federal/us/597/19-1392/, (last visited March 29, 2023).
[29] Roe v. Wade, 410 U.S. 113 (1973), https://supreme.justia.com/cases/federal/us/410/113/, (last visited March 29, 2023).

with a fourth being deterred by passengers.[30] Nearly 3,000 people lost their lives, and the country was struck with grief as it witnessed an unexpected and direct attack on U.S. soil.[31] The U.S. government quickly responded through increased surveillance of U.S. citizens to prevent further attacks. President George W. Bush signed into implementation the P.A.T.R.I.O.T. Act, which gave enormous amounts of authority to the U.S. government.[32] This authority was realized through many aspects: the act permits investigators to utilize already available tools in order to investigate organized crime and drug trafficking; fostered deeper connections (i.e. cooperation and sharing) throughout government agencies; brought the legislature up to date with contemporary technology; and heightened the penalties against those who commit crimes of terrorism.[33] While these are the act's official interpretations, the federal government has more broadly interpreted the act in a manner that benefits their surveillance goals. The act paved the way to the government's access to citizens' private records--financial, medical, Internet, anything that leaves a paper trail--simply on the loose assertion that the request for the records is connected to an ongoing terrorism investigation.[34] By using terrorism as a blanket term, the government technically justified what they were doing in a legal sense but not in an ethical one. As yet another result of the act, any entity forced to turn over records is barred from disclosing this fact to anyone, including the citizen

[30] History.com Editors, September 11 attacks (2010), https://www.history.com/.amp/topics/21st-century/9-11-attacks, (last visited Mar 17, 2023).
[31] *Id.*
[32] USA Patriot Act, National Archives and Records Administration, https://georgewbush-whitehouse.archives.gov/infocus/patriotact/, (last visited Mar 13, 2023).
[33] The USA PATRIOT Act: Preserving Life and Liberty, justice.gov, https://www.justice.gov/archive/ll/highlights.htm#:~:text=Congress%20enacted%20the%20Patriot%20Act,from%20across%20the%20political%20spectrum, (last visited Mar 05, 2023).
[34]ACLU, *Surveillance under the USA/Patriot Act,* American Civil Liberties Union, https://www.aclu.org/other/surveillance-under-usapatriot-act, (last visited Mar 16, 2023).

whose records have been investigated. [35] This means citizens are not even able to challenge these unwarranted searches. The power the P.A.T.R.I.O.T Act granted to the United States government went unchecked, when even something as simple as informing a citizen they're being federally investigated is banned. Even further, the act also allowed for the President to bypass the Foreign Intelligence Surveillance Court (FISC) for surveillance orders when national security is threatened. This court, established by the Foreign Intelligence Surveillance Act (FISA) in 1978,[36] reviews applications for surveillance investigation regarding foreign intelligence[37]. The fact that the President, a singular entity without Congressional approval, could bypass this court only further demonstrates the unethical expansion of the powers of the government under the P.A.T.R.I.O.T. Act.

Naturally, there was some internal opposition to these actions. Two years before these interpretations would be leaked by Edward Snowden, there were elected officials who knew the true extent of surveillance that was occurring. In his 2011 speech to the U.S. Senate regarding the reauthorization of the P.A.T.R.I.O.T. Act, Senator and Intelligence Committee member Ron Wyden stated, "I want to deliver a warning this afternoon: when the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry."[38] The U.S. government utilized a secretive interpretation of the

---

[35] *Id.*

[36] *About the Foreign Intelligence Surveillance Court*, United States: Foreign Intelligence Surveillance Court, https://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court, (last visited Mar 15, 2023).

[37] Foreign Intelligence Surveillance Court | Home, Foreign Intelligence Surveillance Court | United States (2023),https://www.fisc.uscourts.gov/#:~:text=The%20Foreign%20Intelligence%20Surveillance%20Court,actions%20for%20foreign%20intelligence%20purposes, (last visited Mar 18, 2023).

[38] *In speech, Wyden says official interpretations of Patriot Act must be made public*, U.S. Senator Ron Wyden of Oregon (2011), https://www.wyden.senate.gov/news/press-releases/in-speech-wyden-says-official-interpretations-of-patriot-act-must-be-made-public, (last visited Mar 13, 2023).

act, not known by the public, to increase their surveillance while keeping citizens uninformed.[39] Senator Wyden understood intrinsically that this is not what the American people would have wanted or even tolerated. They were left in the dark, the very victims of a surveillance system they did not understand and the full scope of which had not been revealed to them. Senator Wyden goes on to explain how even many members of Congress were in the dark about how the executive branch was interpreting the P.A.T.R.I.O.T. Act since that information is "classified."[40] Even lawmakers of the country were not fully aware of the government's surveillance actions--a dangerous thought considering this is being implemented on all citizens. Coupled with everything discussed above on just how much privacy was violated with the act, there is a clear takeaway: the implementation of the P.A.T.R.I.O.T. Act was deeply unethical and offensive to the ideals of the Constitution.

The surveillance of the late 20th century had already become questionable, but the programs enacted after the September 11 attacks saw the rise of mass surveillance. “Mass surveillance is indiscriminate surveillance. Mass surveillance uses systems or technologies that collect, analyze, and/or generate data on indefinite or large numbers of people instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing.”[41] The fundamental removal of probable cause makes mass surveillance both illegal and unethical.

Edward Snowden

[39] *Id.*
[40] *Id.*
[41] *Mass surveillance*, Privacy International (2023), https://privacyinternational.org/learn/mass- surveillance#:~:text=Mass%20surveillance %20is%20indiscriminate% 20surveillance,is%20reasonable%20suspicion%20of%20wrongdoing, (last visited Mar 7, 2023).

In 2011, President Barack Obama renewed the P.A.T.R.I.O.T. Act and the surveillance authority that came with it.[42] However, the true reach of the bill would be exposed two years later by Edward Joseph Snowden. Snowden was born on June 21st, 1983 in Elizabeth City, North Carolina.[43] Raised in a military family, Snowden almost served himself before he was discharged as a special forces candidate.[44] After his service, his aptitude towards computers made him the ideal candidate for an NSA role in IT, which, in the mid-2000s, was looking to hire more employees with computer knowledge to advance their security measures.[45] Apparently imparting a positive impression, by 2006 Snowden received a job offer from the CIA to work in Geneva, which he accepted. [46] There, even as he benefited from the CIA job, Snowden began to harbor doubts on the morality of his employers by 2008. In February of 2009, Snowden suddenly stepped down from the CIA, getting another position as an NSA contractor in Dell a few short months later. [47]

Meanwhile, Wikileaks, a news company operated by Julian Assange, with information from Chelsea Manning, flipped global opinion of the United States with leaked information on U.S. war practices in the Middle East. From Wikileaks', it is reported that the United States' military was responsible for 109,032 deaths in Iraq, with over sixty

---

[42] *Obama, in Europe, Signs Patriot Act Extension*, NBCNews.com (2011), https://www.nbcnews.com/id/wbna43180202#.Uw1-ojoo7IU, (last visited Mar 15, 2023).
[43] *Edward Snowden*, Encyclopædia Britannica (2023), https://www.britannica.com/biography/Edward-Snowden, (last visited Mar 13, 2023).
[44] *Id.*
[45] Vernon Loeb, *NSA lacks slots, pay to hire top tech talent* , The Washington Post (2000), https://www.washingtonpost.com/archive/politics/2000/07/31/nsa-lacks-slots-pay-to-hire-top-tech-talent/0b09d291-9424-44bb-9f6e-eaaee21b313f/, (last visited Mar 17, 2023).
[46] Edward Snowden, Encyclopædia Britannica (2023), https://www.britannica.com/biography/Edward-Snowden, (last visited Mar 13, 2023).
[47] *Id.*

percent of those being the murder of civilians.[48] This report only added to Snowden's doubts, and he grew increasingly conflicted about exactly who he was working for. Manning's leaks provided Snowden with the motivation to do something about his situation.

The Snowden Files

Now working as a defense contractor in Hawaii at Booz Allen Hamilton with the NSA, Snowden actively searched for information to leak. By 2013, Snowden had the top secret documents he needed to expose the privacy-violating operations of the NSA--he just needed an outlet. In late May 2013, he arrived in Hong Kong, bringing with him four laptops which would give him access to the coveted information.[49] By June 1st, only a few days later, journalists from the Guardian, Glenn Greenwald and Ewen MacAskill, and a documentary developer, Laura Poitras, had made it to Hong Kong as well.[50] Snowden identified himself to the other three and they got to work.[51]

Just four days after the four initially met, the Guardian blasted open the secret U.S.
surveillance by publishing their first article detailing how the U.S. government forced Verizon, an enormous telecommunication company, to disclose millions of Americans' phone records.[52] According to the Guardian's *NSA Files: Decoded*, "Cell phones, laptops, Facebook, Skype, chat-rooms: all allow the NSA to build what it calls 'a pattern of life', a detailed profile of a target and anyone associated with them."[53]

---

[48] Baghdad War Diary, https://wikileaks.org/irq/, (last visited Mar 13, 2023).
[49] Mirren Gidda, *Edward Snowden and the NSA files – timeline*, The Guardian (2013), https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline, (last visited Mar 16, 2023).
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] Ewen MacAskill et al., *NSA files decoded: Edward Snowden's surveillance revelations explained* , The Guardian (2013),

The devices used by most every American citizen were being transformed into a spying device without their knowledge for years. Additionally, the first article revealed the government can collect "telephony metadata" on calls within the US and to the US from other countries. Not only is this a violation of privacy of American citizens but also of citizens from countries outside the U.S., raising more ethical and legal concerns about the United States both on a domestic and international level.

The second story, published just a day after that on June 6th, exposes an NSA program named PRISM, which gives the agency "direct access" to data from social media companies such as Google, Facebook, and Apple.[54] Among the tons of files Snowden exposed, the leaked Powerpoint explaining the program states that PRISM launched its collection of data from Microsoft on September 11, 2007.[55] The types of data include all forms of media: login activity, video conferencing data, transfer of files, data from the cloud, picture, recordings, emails, chat activities, and social media activities. [56]Anything under the Microsoft umbrella--Office products,
Xbox Live, and Hotmail was accessed by PRISM and seen by the NSA.[57] According to these companies, the NSA accessed information without their consent. Violations of privacy rights and unethical, this is a clear

https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/6, (last visited Mar 17, 2023).

[54] Mirren Gidda, *Edward Snowden and the NSA files – timeline,* The Guardian (2013), https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline, (last visited Mar 16, 2023).

[55] *Mass surveillance and terrorism: Does prism keep Americans safer?,* https://trace.tennessee.edu/cgi/viewcontent.cgi?article=3085&context=utk_chanhonoproj, (last visited Mar 16, 2023).

[56] *Id.*

[57] Tayer Houston, *Mass Surveillance and Terrorism: Does PRISM Keep Americans Safer*?, University of Tennessee Honors Thesis Projects, https://trace.tennessee.edu/cgi/viewcontent.cgi?article=3085&context=utk_chanhonoproj, (last visited Mar 16, 2023).

offense against the Fourth Amendment,[58] which protects property unless there is "probable cause" dictating the need to search through property. This offense was made possible through Section 215 of the P.A.T.R.I.O.T Act, which allows for the collection of "'…tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information…'".[59] This one line of legislation allowed the NSA to gather mass information on U.S. citizens' telephony metadata. Utilizing this loophole, the P.A.T.R.I.O.T. Act enabled and the NSA deliberately disobeyed the spirit of the Fourth Amendment by secretly accessing the information from those companies.

Some individuals defend the PRISM program through the justification that it did not target American citizens on purpose. The former Director of National Intelligence, James Clapper, claims PRISM does not "intentionally" target U.S. citizens--that the program is essentially only meant for foreign citizens.[60] However, there is no doubt mass information has been collected on Americans. The NSA just needs to be 51% certain the information does not come from the United States to scrape it from tech companies such as those mentioned above.[61] This essentially means there is no guarantee the NSA won't target U.S. citizens because they are not even 60% confident that the information is foreign-generated. Moreover, the majority of digital information generated in the U.S. goes through multiple servers located outside the U.S., and this is enough justification for the NSA to say the information used and created by

[58] U.S. Const. , art. IV, Constitution Annotated, https://constitution.congress.gov/constitution/article-4/, (last visited March 29, 2023).
[59] Scott F. Mann, *Fact sheet: Section 215 of the USA Patriot Act*, CSIS, https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act, (last visited Mar 16, 2023).
[60] Tayer Houston, *Mass Surveillance and Terrorism: Does PRISM Keep Americans Safer*?, University of Tennessee Honors Thesis Projects, https://trace.tennessee.edu/cgi/viewcontent.cgi?article=3085&context=utk_chanhonoproj, (last visited Mar 16, 2023).
[61] *Id.*

American citizens came from "outside" the U.S.[62] Further, the NSA argues that "if you've got nothing to hide, you've got nothing to fear."[63] But privacy is not a right that is dependent on whether one has something to hide. It would be a stretch to justify the collection of information from foreigners in the name of national security as justified, yet still possible; the NSA's defense crumbles when coupled with the fact it collects an overwhelming amount of information on the U.S.'s own citizens.

This is not the total of what the Snowden files exposed. Not only did the NSA collect private information from systems within the U.S., it also has access to information from close intelligence agencies in other countries.[64] Snowden leaked the existence of the Tempora program, established in 2011 by Britain's GCHQ.[65] Tempora collects mass data of phone and internet activity via fiber-optic cables--data which is in large amounts shared with the NSA.[66] The Snowden files revealed not only the violating practices of the U.S. government, but also of Britain and other U.S. allies, exposing an international network aimed to collect data from individuals who have committed no crime.

Consequences of the Snowden Files

The consequences were immediate and immense. In his 2014 review of the government's surveillance operations, President Obama, while publicly criticizing Snowden for being a traitor, nevertheless emphasized

---

[62] *Id.*

[63] Alex Abdo, *You may have 'nothing to hide' but you still have something to fear*, ACLUA American Civil Liberties Union (2023), https://www.aclu.org/news/national-security/you-may-have-nothing-hide-you-still-have-something-fear, (last visited Mar 29, 2023).

[64] Ewen MacAskill et al., *NSA files decoded: Edward Snowden's surveillance revelations explained* , The Guardian (2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/6, (last visited Mar 17, 2023).

[65] *Id.*

[66] *Id.*

the need to heavily reconsider the NSA operations. He states, "We have to make some important decisions about how to protect ourselves and sustain our leadership in the world, while upholding the civil liberties and privacy protections that our ideals and our Constitution require." [67] Going forward, Obama outright said the government must maintain the "civil liberties" and "privacy protections" that are core to the ideals of the United States. This would have an enormous impact. As a result of Snowden's leak, the NSA now operates under thorough congressional and executive branch oversight.[68]

In 2015, the F.R.E.E.D.O.M. Act was passed which banned mass collection of data and provided other regulations.[69] While some would argue that this extreme surveillance that emerged from the P.A.T.R.I.O.T. Act is no longer in place due to the F.R.E.E.D.O.M. Act, this is not a guarantee. For years after 9/11, citizens had no idea they were being closely monitored by their government. It was not until the release of the Snowden files that the PRISM program and more came to light. Even now, we are still not fully aware of what the NSA was doing that the Snowden files did not report because much of it remains classified. Further, we do not know how the government is interpreting the F.R.E.E.D.O.M Act, just as we did not know how they were interpreting the P.A.T.R.I.O.T. Act. The lack of transparency, proven misuse, and valid distrust over government surveillance should not be taken lightly. It is important to remain skeptical of what programs are occurring since it would not be the first time the government has lied about surveillance.

---

[67] *Remarks by the president on review of Signals Intelligence*, National Archives and Records Administration, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence, (last visited Mar 14, 2023).

[68] *Id.*

[69] Jake Laperruque, *The history and future of mass metadata surveillance*, Project On Government Oversight (2019), https://www.pogo.org/analysis/2019/06/the-history-and-future-of-mass-metadata-surveillance, (last visited Mar 29, 2023).

U.S. technology companies, too, experienced some backlash from the leak. While domestically not much changed, foreign markets seemed to harbor suspicions against U.S. tech companies.[70] Both Microsoft and Amazon reported the loss of international clients after the revelations.[71] This wariness is not-unfounded given that the leak revealed the U.S. used those companies to spy on individuals both domestically and internationally.

The fight against terrorism, too, might have been impaired. After Snowden's leaks, terrorist organizations then had information on how they were being surveilled, meaning they could potentially thwart this surveillance. James Clapper, Director of Intelligence, cautioned that revealing the NSA's programs to United States enemies harmed America's capacity to stop another 9/11 from happening, claiming the leak to be "the most destructive [bleeding] of American secrets in history."[72] Snowden became a divisive figure, to some he was a hero for revealing the American government's mass surveillance, while others villainized and called him a traitor due to the potential disastrous consequences of his leak.

For Snowden himself, the consequences of his actions would leave him scrambling. He was charged with two counts of espionage and one count of robbery of federal property.[73] Fleeing from these charges, he sought asylum in Russia for eight years. Then, on September 26th, 2022,

---

[70] James A. Lewis, Denise E. Zheng , William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data, Appendix A* (2017), Center for Strategic and International Studies , https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data, (last visited March 29, 2023).

[71] *Id.*

[72] *Edward Snowden, the NSA mass surveillance* , Constitutional Rights Foundation (2016), https://www.crf-usa.org/images/pdf/gates/snowden_nsa.pdf , (last visited Mar 14, 2023).

[73] U.S. v. Edward J. Snowden, Case No. 1:13 CR 265 (CMH) (under seal) (E.D.Va. 2013), https://sgp.fas.org/jud/snowden/complaint.pdf United States of America vs Edward J. Snowden, (2013), (last visited Mar 14, 2023).

Snowden achieved Russian citizenship.[74] Despite his residency in Russia, however, Snowden claimed he would come back if he was promised a fair trial. Unfortunately, that is not the case. In 2019, six years after living in Russia, he stated, "And of course I would like to return to the United States. That is the ultimate goal. But if I'm going to spend the rest of my life in prison, the one bottom-line demand that we all have to agree to is that at least I get a fair trial. And that's the one thing the government has refused to guarantee because they won't provide access to what's called a public interest defense." [75] Even if it meant going to prison, Snowden would return to the United States if given a fair trial, but the government declines to ensure this will happen, and as such, as a very consequence of revealing the government's secrets, Snowden has remained away from his home since his world-shaking revelations.

Violations of the Fourth Amendment's Right to Privacy

The word "privacy" is not one used in the U.S. Constitution. This is mainly because the U.S. has the oldest Constitution in the world dating back to 1787. However, interpreting this brief document that is at the center of American law and protections is essential to understanding why this surveillance is ultimately illegal. The central legal argument for privacy centers around the interpretation of the Fourth Amendment.

The Fourth Amendment of the Constitution states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the

[74] Charles Maynes, *Putin grants Russian citizenship to Edward Snowden,* NPR (2022), https://www.npr.org/2022/09/26/1125109303/putin-edward-snowden-russian-citizenship, (last visited Mar 14, 2023).

[75] Devan Cole, *Edward Snowden says he would like to return to the US if he is guaranteed a fair trial,* CNN (2019), https://www.cnn.com/2019/09/17/politics/edward-snowden-russia-us-fair-trial/index.html , (last visited Mar 14, 2023).

persons or things to be seized."[76] At the time of its creation, this amendment protected the private property of an individual from being intruded upon by the government, unless there was reasonable suspicion.[77] However, the digital age brings about new questions as to what private property may be. The amendment specifically utilizes the word "effects" which refers to items that individuals own, including technology. Thus, these digital items should be protected from surveillance, but this has thus far not been respected by the government.

The Fourth Amendment also establishes a need for "probable cause," something long missing in the action after the September 11 attacks. The PRISM program alone hands over personal data and communications to the government without question.[78] Whether under suspicion or not, everyone is subject to these surveillance programs. If individual data is taken for no justifiable reason, besides prevention of a terrorist attack that may never come, then every American citizen becomes a suspect of terrorism to conspire against the U.S. government. This is not a reasonable way to prevent terrorism, it is invasive of citizens personal information, and most of all a clear violation of the Fourth Amendment.

The Supreme Court has had difficulty in determining the allowances of privacy, at times flipping back and forth. For example, the 1967 case of *Katz v. United States* establishes that the Fourth Amendment includes protections against wiretapping.[79] The police had recorded a call of Katz's to gather evidence for a crime, but this case made its way to the Supreme Court who decided that evidence gathered this way could not

[76] Brian Smentkowski, *Fourth Amendment*, Encyclopedia Britannica (2023), https://www.britannica.com/topic/Fourth-Amendment, (last visited Mar 29, 2023).
[77] *Id.*
[78] Tayler Houston, *Mass surveillance and terrorism: Does PRISM keep Americans safer?*, University of Tennessee Honors Thesis Projects, https://trace.tennessee.edu/cgi/viewcontent.cgi?article=3085&context=utk_chanhonoproj, (last visited Mar 16, 2023).
[79] Katz v. United States, 389 U.S. 347 (1967), Justia, https://supreme.justia.com/cases/federal/us/389/347/, (last visited Mar 29, 2023).

be administered.[80] The ruling specifically states, “Indeed, we have expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements, overheard without any ‘technical trespass under . . . local property law. Once this much is acknowledged, and once it is recognized that the Fourth Amendment protects people -- and not simply "areas" -- against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.”[81] Here, the court establishes that the Fourth Amendment is not bound by property, rather it is a right that binds the government from intruding on the privacy of an individual. This ruling when applied to the digital age means that the government cannot monitor citizens in order to gather evidence of terrorism without due process and probable cause.

In more recent cases, the Supreme Court has upheld the notion of privacy. In the 2001 case of *Kyllo v. United States*, the court looked at the use of technology in surveillance.[82] Kyllo was suspected of growing marijuana in his home and the authorities confirmed this suspicion by using thermal-imaging technology.[83] However, Kyllo argued that this was a violation of the Fourth Amendment's protection of searches. The court agreed and said, “...the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.”[84] By deeming that use of technology that is not widely available constitutes a search, then the mass

[80] *Id.*
[81] *Id.*
[82] Kyllo v. United States, 533 U.S. 27 (2001), Justia, https://supreme.justia.com/cases/federal/us/533/27/, (last visited March 29, 2023).
[83] *Id.*
[84] *Id.*

surveillance technology, connections, and access the government has on individuals is entirely unconstitutional.

In the 2014 case of *Riley v. California*, authorities had looked at phone records of Riley without a warrant and he was charged in association with gang crimes.[85] Typically, police can look through personal belongings with incident-to-arrest being the exception to warrants. However, in this case, the Supreme Court made it clear that accessing information on a person's phone did not count under this because there is too much personal information on the phone.[86] The court specifically states, "The fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely. Not every search 'is acceptable solely because a person is in custody.'"[87] This case established that law enforcement does not have access to technology without a warrant, yet the government has been collecting information from technology constantly. Furthermore, suspicion of potential terrorists is far too broad to constitute mass surveillance on the American people, and as mentioned by the court, searches are not reasonable without reasonable suspicion.

Furthermore, in 2018 in the case *Carpenter v. United States*, the court reinforced this decision with their ruling that a warrant is needed to access location data generated by phones.[88] Carpenter's location data was used to connect him to a crime because location data is typically held by a third party, due to this there is no expectation of privacy given to these companies.[89] Furthermore, the court ruled that a search warrant is needed to access this location data, saying, "...the fact that such information is gathered by a third party does not make it any less deserving of Fourth

[85] Riley v. California, 573 U.S. 373 (2014), Justia, https://supreme.justia.com/cases/federal/us/573/373/, (last visited March 29, 2023).
[86] *Id.*
[87] *Id.*
[88] Carpenter v. United States, 585 U.S. ___ (2018), Justia, https://supreme.justia.com/cases/federal/us/585/16-402/, (last visited March 29, 2023).
[89] *Id.*

Amendment protection."[90] A person's location is a personal matter and cannot be carelessly handled. Yet, the PRISM program collected this third party data without the knowledge or consent of those being surveilled. This reinforces the protection of privacy in the eyes of the court, yet for years the U.S. government breached such expectations.

Most clearly, in the case of *United States v. Moalin* in 2020, what Snowden revealed was deemed unconstitutional.[91] The case was filed in 2013, but it took seven years for it to reach a conclusion due to the classified information involved. The Ninth Circuit deemed that the Somali defendants would still be convicted through evidence found through this data collection, but the court did relent saying, "The panel held that the government may have violated the Fourth Amendment when it collected the telephony metadata of millions of Americans…"[92] The opinions of these courts upholds that these surveillance programs were a violation of the Fourth Amendment, and thus it was undoubtedly unconstitutional.

Conclusion

In no uncertain terms, the surveillance upon American citizens has been a violation of established Fourth Amendment protections, yet Americans remain fully aware of what is truly occurring. Much of these surveillance programs remain classified, so the full scope or continuous use of them is unknown. Greater transparency and regulation is needed for the government to be trusted with surveillance.

[90] *Id.*
[91] United States v. Moalin, No,.13-50572 (S.D. Ca, 2020), American Civil Liberties Union (2023), https://www.aclu.org/legal-document/united-states-v-moalin-ninth-circuit-opinion, (last visited Mar 29, 2023).
[92] *Id.*