A History of Privacy Rights in America

From the Fourth Amendment to the Patriot Act

By William Twomey '19

This analysis will trace the development of privacy rights in the United States, beginning with the ratification of the Bill of Rights and ending with the passage of the Patriot Act in 2001. Twomey explores the original constitutional understanding of privacy, tracks the judicial incorporation of privacy as a constitutionally guaranteed right, analyzes how new technologies posed difficult questions for the courts and the legislature, and examines the state of privacy rights directly following the September 11th attacks. This analysis will pay special attention to the Electronics Communications Privacy Act of 1986 (ECPA) and the Foreign Intelligence Surveillance Act of 1978 (FISA) and how these two pieces of legislation altered the state of Americans' privacy rights in the electronic age.

The history of privacy rights in the United States begins with the ratification of the Bill of Rights in 1791. An effort spearheaded by James Madison, the passage of the Bill of Rights offered new protections for the American people from overreach by the newly formed (and much more centralized) federal government. It included specific guarantees of personal freedoms and rights and placed clear limitations on the federal government's power. One such protective amendment, and the one this analysis will focus on, is the Fourth Amendment. In general, the Fourth Amendment prohibits the unreasonable and unwarranted searches and seizures so common in the Colonies under British dominion. It also protects against arbitrary arrests and is the basis of American law regarding search warrants, stop-and-frisk, safety inspections, and wiretaps and other forms of surveillance. As Daniel Solove explains:

> [The Fourth Amendment] ensures that the government cannot gather information about you without proper oversight and limitation…It requires that the government justify to a court why it has a compelling reason to be interested in your information.[1]

The text of the Fourth Amendment to the United States Constitution reads as follows:

> The right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[2]

Originally, the Fourth Amendment enforced the notion that "each man's home is his castle," secure from unreasonable searches and seizures of property by the government. But over the course of American history, the Supreme Court has delivered several rulings that have transformed the meaning of the Fourth Amendment to apply to modern technology available to law enforcement and the federal government. In these cases, it has generally been decided by the Court that an officer or agency must demonstrate to a judge that there exists "probable cause" to search or seize property and can only engage in that search or seizure upon attaining a warrant. According to the Legal Information Institute at Cornell University Law School, probable cause exists when there is "a reasonable basis for believing that a crime may have been committed (for an arrest) or when evidence of the crime is present in the place to be searched (for a search)."[3] However, cases of "exigent circumstances" (circumstances in which a law enforcement officer has a probable cause but no sufficient time to secure a warrant) may justify a warrantless search or seizure. Probable cause was enshrined in judicial doctrine in 1983 in *Illinois v. Gates*, 462 U.S. 213 in which the Court viewed it as a "practical, non-technical" judgment that calls upon the "factual and practical considerations of everyday life on which reasonable and prudent men act."[4]

For acting as the Amendment that safeguards Americans' privacy, something is notably lacking from the text of the Fourth Amendment: the word "privacy" is never mentioned. In fact, nowhere in the Bill of Rights, or anywhere in the Constitution, is a discussion of privacy or privacy rights present. The first real mention of a fundamental "right to privacy" in the American legal community is in an article published in the *Harvard Law Review* in 1890 by Samuel Warren and Louis Brandeis entitled "The Right to Privacy." In it, Warren and Brandeis argue for what they call "the right to be let alone,"[5] and argue for the existence of the fundamental principle that "the individual shall have full protection in person and in property."[6] The article immediately received a strong reception and continues to be a

touchstone of modern discussions of privacy law.

The next chapter in the history of American privacy rights comes from the Supreme Court in the case *Olmstead v. United States,* 277 U.S. 438 (1928). New technology had brought about new questions regarding citizens' privacy, the meaning of probable cause, and the right of government agencies to access citizens' information. The plaintiff in the case, Roy Olmstead, was a suspected bootlegger. Without judicial approval, federal agents installed wiretaps in the basement of Olmstead's building and in the streets near his home. Olmstead was convicted with evidence obtained from the wiretaps. Olmstead petitioned, and his case eventually reached the Supreme Court. The question before the Court was: did the use of evidence disclosed in wiretapped private telephone conversations violate the recorded party's Fourth Amendment rights? In a 5-4 decision, the Court ruled against Olmstead. In the majority opinion, Justice William Howard Taft wrote:

> [The Fourth Amendment] does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.[7]

The Supreme Court understood privacy violations as physical intrusions, and because the evidence obtained was provided by devices installed outside of Olmstead's home, it did not involve a physical trespass onto Olmstead's property.

Though this may seem like a defeat for privacy rights, it is not uncommon for some of the foundations of American legal theory to be found in the dissents of overturned cases, and *Olmstead* is no different. In his dissent, Justice Louis Brandeis (one of the authors of "The Right to Privacy") argued that the Court's threshold for determining Fourth Amendment coverage was myopic and antiquated. He argued that the Fourth Amendment must have "the capacity of adaptation to a changing world." In a now-famous passage of his dissent, Justice Brandeis wrote:

> …subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[8]

Today, Justice Brandeis' words sound prophetic. The "subtler and more far-reaching" methods of surveillance that he warned of in 1928 are eerily reminiscent of current technologies that allowed the widespread NSA surveillance of citizens after 9/11, which I will cover in detail later in this analysis.

> Katz was entitled to Fourth Amendment protection for his conversations and that a physical intrusion into the area he occupied was unnecessary to bring the Amendment into play.

As the *Olmstead* case demonstrated, focusing on physical intrusions was an outmoded way to determine the scope of Fourth Amendment protection. Unless the Court modernized its test for determining when the Fourth Amendment would apply, it would become effectively obsolete. This modernization finally came forty years later, in *Katz v. United States*, 389 U.S. 347 (1967). Acting on a suspicion that Katz was transmitting gambling information over the phone to clients in other states, federal agents installed an eavesdropping device in a public

phone booth used by Katz. Based on recordings of his end of the conversations, Katz was convicted. On appeal, Katz argued that the recordings could not be used as evidence against him. The question before the Court was: does the Fourth Amendment protection against unreasonable search and seizures require the police to obtain a search warrant in order to wiretap a public pay phone? In a 7-1 decision that overturned the *Olmstead* ruling, the Court ruled that Katz was entitled to Fourth Amendment protection for his conversations and that a physical intrusion into the area he occupied was unnecessary to bring the Amendment into play. In the majority opinion, Justice Potter Stewart outlined the dramatic shift in judicial doctrine concerning privacy:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposed 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.[9]

In a concurring opinion, Justice John Marshall Harlan explained that the Fourth Amendment should apply whenever a person exhibits an "actual (subjective) expectation of privacy" that "society is prepared to recognize as 'reasonable'."[10] The "reasonable expectation" that Justice Harlan mentioned gave birth to the "reasonable expectation of privacy test," which protects people from warrantless searches of places or seizures of objects that have a subjective expectation of privacy that is deemed reasonable in public norms.[11] With one decision, the Court had successfully incorporated the right to privacy, previously a theoretical right, into American law. It took nearly eight decades, but the fundamental "right to be let alone" discussed by Brandeis and Warren in 1890 had finally been made law.

With the right to privacy now enshrined in the courts, it was time for the legislature to act. With technology rapidly changing, it soon became clear that the next arena of privacy rights litigation would involve electronic information. The legislature passed two bills in the twentieth century that further regulated the federal government's ability to surveil its civilians. These were the Foreign Intelligence Surveillance Act of 1978 (FISA) and the Electronic Communications Privacy Act of 1986 (ECPA). Both FISA and the ECPA were meant to update surveillance laws with new technology in mind, but were drafted in the years just prior to the internet age. The advent of the internet and a new interconnected, global society rendered many of the provisions of these acts obsolete. The Patriot Act of 2001 took advantage of these discrepancies, as will be discussed later.

The first act of Congress to address citizens' electronic right to privacy was FISA, passed after two congressional investigations found that the executive branch had consistently abused its power and conducted domestic electronic surveillance unilaterally against journalists, civil rights activists, members of Congress, and others in the name of national security. Mindful of the threat unchecked electronic surveillance posed to Americans' privacy, Congress strictly limited FISA's scope so that it could only be used if the "primary purpose" of government surveillance of Americans was the gathering of foreign intelligence.[12] The abbreviated purpose of the original act reads as follows:

> …to erect a secure framework by which the executive branch could conduct legitimate electronic surveillance for foreign intelligence purposes within the context of this Nation's commitment to privacy and individual rights.[13]

Additionally, the Attorney General established a set of guidelines for FBI investigations in

1976.[14] The Central Intelligence Agency (CIA) was the chief beneficiary of FISA and used the guidelines to gather foreign intelligence on foreign agents on American soil. FISA surveillance orders (the equivalent of a judge-issued warrant) are obtained from the Foreign Intelligence Surveillance Court, or FISC. The proceedings of the FISC, however, are entirely secret. There are no reports, transcripts, or public records available from the FISC, so the manner in which it decides who is eligible for electronic surveillance is largely unknown. When the Patriot Act amended FISA in 2001, the limitations on who could be surveilled were greatly weakened, but the FISC remained unchanged. Furthermore, foreign-intelligence-gathering standards are much more lax than criminal or domestic standards. As Hina Shamsi, director of the American Civil Liberties Union's National Security Project explains:

> Under the Foreign Intelligence Surveillance Act (FISA), the government need not show suspicion of wrongdoing, and it can conduct electronic and covert searches domestically if the target of these searches is 'foreign-intelligence information' from a foreign power or an agent of a foreign power.[15]

The next piece of legislation that regulates electronic surveillance of civilians is the Electronic Communications Privacy Act, or ECPA, passed in 1986. At its core, the ECPA regulates wiretapping, bugging, and searches of computers, among other things. The law aimed to provide privacy protection of email, stored computer files, and communications records. It requires government officials to justify their belief that the surveillance will uncover evidence of a crime, as well as explain to a court why alternative investigative methods would be ineffective, much like a normal, criminal investigation involving search warrants for physical places. One major flaw of the ECPA, however, is that the so-called "exclusionary rule" does not apply. The exclusionary rule is a judicial doctrine first outlined in *Mapp v. Ohio*, 367 U.S. 643 (1961) and later expanded in *Miranda v. Arizona,* 384 U.S. 439 (1966). It mandates that evidence gathered from an unreasonable search or seizure in violation of the Fourth Amendment or an improperly elicited self-incriminatory statement be excluded from court.[16] It therefore protects accused persons from being convicted based on illegally obtained evidence. Though it is one of the strongest protections of Americans' constitutional rights, the exclusionary rule does not apply to evidence obtained under the ECPA. When the ECPA was amended under the Patriot Act, the exclusionary rule was again omitted from the substance of the law.

There are no reports, transcripts, or public records available from the FISC, so the manner in which it decides who is eligible for electronic surveillance is largely unknown.

Before the passage of the Patriot Act, FISA and the ECPA operated largely within their own respective spheres, kept separate by the strict limits present in FISA's scope. Under the amendments to these laws in the Patriot Act, however, this "wall" between government surveillance for domestic law enforcement purposes and surveillance activities for foreign-intelligence gathering was dismantled almost entirely. This led to widespread domestic surveillance on Americans, with almost no attention to foreign allegiance or foreign contacts. In essence, it completely voided the original purpose of FISA. With the added expansion of the ECPA, the government's ability to surveil its citizens increased tremendously.

After the 9/11 attacks, the state of citizens' electronic privacy changed tremendously. With both a judicial as well as a legislative conception of privacy rights in mind, I will now begin a discussion regarding how the Patriot Act updated, and in some ways rolled back, protections of citizens' electronic privacy.

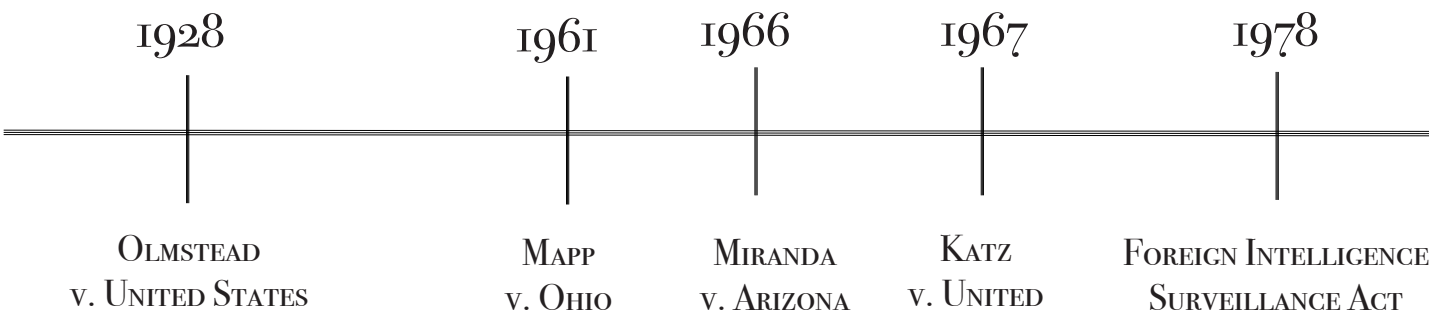
H.R. 3126: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 was signed into law by President George W. Bush on October 26th, 2001, just forty-five days after the Twin Towers fell. The final preamble of the bill reads as follows:

> An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.[17]

The Act gave law enforcement permission to search a home or business without the owner's or the occupant's consent or knowledge, expanded the powers of the Federal Bureau of Investigation (FBI) to search telephone, e-mail, and financial records without a court order, and, perhaps most notably, granted immense freedom to the National Security Agency (NSA) to collect domestic and international communications of Americans without a warrant based on probable cause. The Act also greatly expanded and altered the provisions of both the ECPA and FISA, the two greatest legislative protections for Americans' electronic privacy.

Though many provisions of the Patriot Act became controversial, I will focus primarily on Title II, titled "Enhanced Surveillance Procedures," which made substantial amendments to FISA and the ECPA. Focusing here will be the most useful because of our earlier discussions of both FISA and the ECPA. It covers all aspects of the surveillance of suspected terrorists, those suspected of engaging in computer or fraud abuse, and agents of a foreign power who are engaged in clandestine activities. This section allowed the government of the United States to gather "foreign intelligence information" from both U.S. and non-U.S. citizens, and substantially changed the meaning and purpose of FISA.

The first problematic section of the Patriot Act is Section 206: "Roving Surveillance Authority Under the Foreign Intelligence Surveillance Act of 1987." As its title suggests, this section greatly diminished the limitations placed on FISA and greatly increased the surveillance capabilities of the federal government. As previously stated, typical judicial orders authorizing wiretaps identify the person or place to be monitored. This requirement has its roots firmly planted in the Fourth Amendment, wherein it calls for warrants "particularly describing the place to be searched, and the persons of things to be seized."[18] However, these "roving" or multipoint warrants are not required to specify the person nor the place to be surveilled. Roving wiretaps are unique because they follow a target rather than a specific device. For example, before its amendment under the Patriot Act, FISA required that a separate surveillance application be submitted to the FISC each time a target switched from pay phone to cell phone, email to Blackberry, etcetera. Under the Patriot Act, the Court could order surveillance focused on the



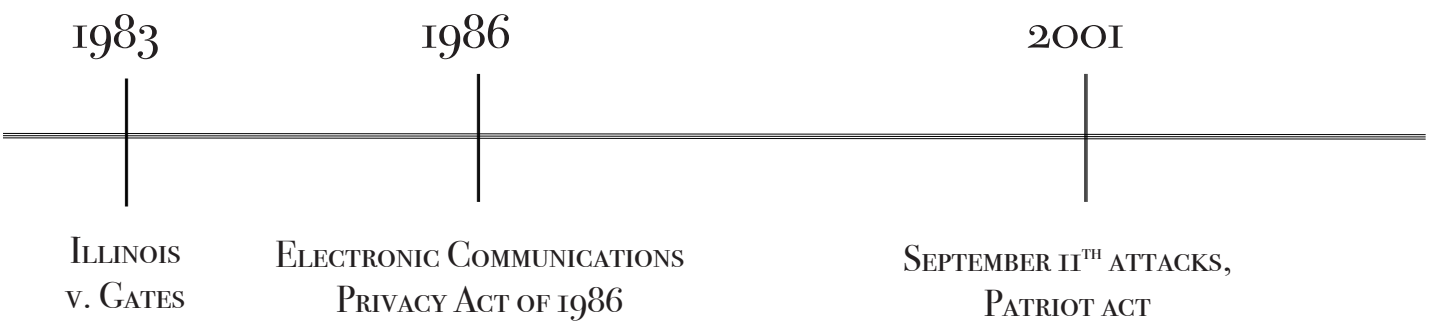
target, "rather than the device he or she is using when 'the actions of the target of the application may have the effect of thwarting the identification' of a specific device."[19] Furthermore, under FISA, the government need not always identify a target to obtain a warrant. FISA section 105(c)(1)(A) requires that an order specify "the identity, if known, or a description of the target of the electronic surveillance." Therefore, when combined with the new roving authority under the Patriot Act, the federal government may obtain an order to conduct surveillance that specifies neither a named target nor a specific device to tap.

Many critics argue that Section 206 of the Patriot Act violates the Fourth Amendment because the new roving wiretaps need not describe "the place to be searched, and the things to be seized." In *Katz*, the Court decided that wiretapping did indeed constitute an act of searching. Thus, many legal scholars argue that a roving wiretap warrant that does not specify the place (or device) to be searched or identify the individual to be surveilled is a violation of citizens' Fourth Amendment rights.

The next problematic section is Section 213: "Authority for Delaying Notice of the Execution of a Warrant." Before the Patriot Act, criminal search warrants required prior notification except in exigent circumstances or for stored communication when advanced notice would "seriously jeopardize investigation."[20] The Patriot Act expanded this once narrow loophole–used solely for stored communications–to all searches. Federal agents could now use so-called "sneak and peek searches" to circumvent the Fourth Amendment by conducting searches of both physical places as well as stored communications without notifying the searched party of the execution of a warrant. This loophole also allows federal agents to use FISA orders, which are supposedly reserved for foreign intelligence gathering, to gather evidence in domestic, criminal investigations. Furthermore, these sneak-and-peek warrants are not limited to terrorism cases, thereby calling into serious question the justification that the searches are conducted because of circumstances that would "seriously jeopardize investigation." In fact, for the 2007 fiscal year, the federal government reported that out of 690 sneak-and-peek applications, only seven were used for terrorism cases.[21]

Out of 690 sneak-and-peek applications, only 7 were used for terrorism cases.

Many constitutional scholars and activists argue that Section 213 violates the Fourth Amendment protection from unreasonable searches and seizures. Federal agents can abuse this loophole to conduct illegal, secret searches without prop-

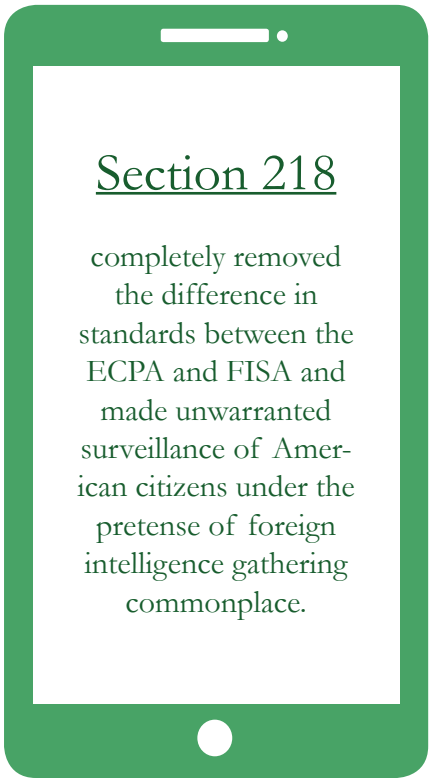


er probable cause or notification of the searched party. This can lead to innocent citizens being searched without being notified and without reason. In 2006, Brandon Mayfield, an American attorney from Portland, Oregon, was subjected to secret FISA searches of his home and office after an FBI agent mistakenly identified his fingerprint on materials related to a terrorist bombing in Madrid, Spain. Mayfield challenged the constitutionality of the Patriot Act provision that allows FBI agents to use FISA orders (supposedly reserved for foreign intelligence gathering) to gather evidence in a criminal investigation. An initial ruling from the Ninth Circuit Court of Appeals declared several provisions of the Patriot Act (including 213) unconstitutional, but the United States government appealed, and the ruling was overturned.

The next contentious section of the Patriot Act is Section 218: "Foreign Intelligence Information." This section, though brief, has had a profound impact on the jurisdiction and implementation of FISA. Because of its brevity, it is transcribed here in full:

> Sections 104(a)(7)(B) and section 303(a)(7)(B) (U.S.C. 1804(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking "the purpose" and inserting "a significant purpose."[22]

As previously stated, FISA's original text required that the "primary" purpose of a FISA search or surveillance must be to gather foreign intelligence. The Patriot Act eliminated this requirement. Under the Patriot Act's amendment in Section 218, the government need only show that a "significant purpose" of the search or surveillance is to gather foreign information in order to obtain authorization from the FISC. This seemingly minor change allows the government to use FISA to circumvent basic protections of



the Fourth Amendment, even where criminal prosecution is the government's primary motive for conducting the search or surveillance. This allows the government to conduct investigations to gather evidence for use in criminal trials without establishing probable cause of illegal activity before a neutral and disinterested magistrate, and without providing the notice required with ordinary warrants (as enumerated in Section 213's "sneak-and-peek searches"). Furthermore, the FISC must accept the government's assertion that the target of surveillance is "an agent of a foreign power" unless the charge is "clearly erroneous."

Section 218 of the Patriot Act is controversial because it lowers the evidentiary standards for obtaining a warrant in otherwise normal crimnal investigations. The amendment completely removed the legal "wall" discussed earlier between criminal investigations (regulated by the ECPA) and surveillance for the purposes of gathering foreign intelligence information (regulated by FISA). FISA and the ECPA have different standards because the threats they deal with are of different imminence and gravity. The ECPA requires proof of probable cause, a court-issued warrant, and prior notification of the obtaining of that warrant to conduct surveillance with the intent of gathering evidence for criminal investigations. FISA standards were made lower (but still reasonable enough to protect innocent citizens from unwarranted surveillance) because cases of espionage involving agents of a foreign power are more serious and require more immediate action by the authorities. Section 218 completely removed the difference in standards between the ECPA and FISA and made unwarranted surveillance of American citizens under the pretense of foreign intelligence gathering commonplace.

The history of privacy rights in America is a rich and complex one, ebbing and flowing with monumental historical events. Though the "right to privacy" did not make it into the Constitution verbatim, the Framers sowed the seeds of this right in their protection from unreasonable searches and seizures present in the Fourth Amendment. Through the legal genius of Justice Brandeis, this now-fundamental right transformed from a legal theory published in a *Harvard Law Review* article to a fully incorporated and enforceable civil liberty in Katz. The twentieth century posed new challenges and questions regarding privacy in an increasingly electronic world, and the legislature did its duty by updating laws to meet the standards of judicial doctrine. In the face of new threats, most notably the scourge of global terrorism, the legislature again acted by passing the Patriot Act. In doing so, it passed legislation that, in some cases, lacked clear constitutional grounds. Though Congress may have had Americans' best interest in mind, we have seen the Act come under fire from both sides of the aisle, and some provisions of the Act go contrary to the rulings of the Court. The story of privacy rights in America is not unique, but it does show both the beauty and the danger of the American federal system. At its best, the legislature and the judiciary work in tandem, ensuring security but never compromising liberty; however, as we have seen with the Patriot Act, the two branches are no strangers to conflict.

Endnotes

1. Daniel Solove, Nothing to Hide: The False Tradeoff between Privacy and Security (New Haven: Yale University Press), 93.
2. The Fourth Amendment to the United States Constitution
3. "Probable Cause," Wex Legal Dictionary, Legal Information Institute, Cornell University Law School, https://www.law.cornell.edu/wex/probable_cause
4. Illinois v. Gates, 462 U.S. 213 (1983)
5. Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, Vol. 4, No. 5 (The Harvard Law Review Association: 1890)
6. Warren and Brandeis
7. Olmstead v. United States, 277 U.S. 438 (1928)
8. Ibid.
9. Katz v. United States, 389 U.S. 347 (1967).
10. Ibid.
11. "Expectation of Privacy," Wex Legal Dictionary, Legal Information Institute, Cornell University Law School, https:/www.law.cornell.edu/wex/expectation_of_privacy
12. "Reclaiming Patriotism: A Call to Reconsider the Patriot Act." American Civil Liberties Union, published March 2009, https://www.aclu.org/sites/default/files/pdfs/safefree/patriot_report_20090310.pdf
13. Solove, Nothing to Hide, 10
14. Office of the Attorney General, U.S. Department of Justice, Domestic Security Investigation Guidelines (1976).
15. Hina Shamsi and Alex Abdo, "Privacy and Surveillance Post-9/11," Human Rights Magazine (Chicago: American Bar Association Publishing, 2011) http://www.americanbar.org/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11.html
16. "Exclusionary Rule," Wex Legal Dictionary, Legal Information Institute, Cornell University Law School, https://www.law.cornell.edu/wex/exclusionary_rule
17. H.R. 3162 – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 https://www.congress.gov/bill/107th-congress/house-bill/3162/text
18. Fourth Amendment to the United States Constitution
19. Stewart A. Baker and John Kavanagh, Patriot Debates: Excerpts Debate the USA PATRIOT Act, "Section 206: Roving Surveillance Authority under FISA," (Chicago: American Bar Association Publishing, 2005) https://apps.americanbar.org/natsecurity/patriotdebates/section-206
20. Section 3103a, Title 18, United States Code
21. "Reclaiming Patriotism: A Call to Reconsider the Patriot Act," https://www.aclu.org/sites/default/files/pdfs/safefree/patriot_report_20090310.pdf
22. United States Cong. House. H.R. 3162 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 107th Cong. 1st Sess. 2001. Government Publishing Office, https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

REFERENCES

H.R. 3162 – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 https://www.congress.gov/bill/107th-congress/house-bill/3162 text

Illinois v. Gates, 462 U.S. 213 (1983)

Katz v. United States, 389 U.S. 347 (1967)

Office of the Attorney General, U.S. Department of Justice, Domestic Security Investigation Guidelines (1976)

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

"Reclaiming Patriotism: A Call to Reconsider the Patriot Act." American Civil Liberties Union, published March 2009, https://www.aclu.org/sites/default/files/pdfs/safefree/patriot_report_20090310.pdf

Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," Harvard Law Review, Vol. 4, No. 5 (The Harvard Law Review Association: 1890)

Shamsi, Hina and Alex Abdo, "Privacy and Surveillance Post-9/11," Human Rights Magazine. Chicago: American Bar Association Publishing, 2011 http://www.americanbar.org/publications/human_rights_magazine_home/human_rights_vol38_2011/human_rights_winter2011/privacy_and_surveillance_post_9-11.html

Solove, Daniel. Nothing to Hide: The False Tradeoff between Privacy and Security. New Haven: Yale University Press, 2011.

Baker, Stewart A. and John Kavanagh, Patriot Debates: Excerpts Debate the USA PATRIOT Act, "Section 206: Roving Surveillance Authority under FISA," (Chicago: American Bar Association Publishing, 2005) https://apps.americanbar.org/natsecurity/patriotdebates/section-206

United States Code, Section 3103a, Title 18

United States Cong. House. H.R. 3162 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 107th Cong. 1st Sess. 2001. Government Publishing Office, https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

Wex Legal Dictionary, Legal Information Institute, Cornell University Law School, published 1992, https://www.law.cornell.edu/wex/probable_cause