THE TENSION BETWEEN MODERN TECHNOLOGY AND THE LEGAL FOUNDATIONS OF PRIVACY

by

LIAM J. VLAMING

A THESIS

Presented to the Department of Political Science
and the Robert D. Clark Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Science

December 2017

An Abstract of the Thesis of

Liam J. Vlaming for the degree of Bachelor of Science
in the Department of Political Science to be taken December 2017

The Tension Between Modern Technology and the Legal Foundations of Privacy

Approved: _____

John Davidson

The goal of this thesis is to explore the legal foundations of privacy and analyze the ways in which societal and technological advancements have influenced the progression of privacy rights. With regard to the significant breadth of privacy issues, the scope of this thesis is narrowed to primarily focus on the informational aspects of privacy along with some analysis of physical seclusion as it relates to the confidentiality of the details of one's personal life.

Beginning with the Fourth Amendment and moving through an analysis of Supreme Court decisions, I establish a timeline of how the right to privacy developed and what forces were most influential in shaping its trajectory. I also examine the legal doctrines that are currently guiding privacy rights, and I explore the ways in which they are succeeding or failing to address the norms and expectations of individuals in the digital age. These include issues that are presently arising in the areas of large scale data collection, increased connectivity and information sharing, and national security. I explore the foundational causes of issues in these areas as well as their lasting effects, both tangible and psychological.

Through my exploration of the existing jurisprudence, I analyze the factors that shaped the development of privacy rights. I use this historical background in assessing the current issues facing the future of privacy protections. I identify four areas of particular concern: (1) the increasingly difficult balance of privacy and security, (2) the inadequate adaptation of aging legal doctrines, (3) troubling issues of access to information, including the disproportionate access that the government and certain business entities have relative to most private individuals, combined with trends toward further consolidation of information and the entanglement of government surveillance programs with private information gathering which will further widen the divide as well as diminish transparency, (4) and finally, the changing psychological aspects of privacy. In addressing each of these areas, I identify causes, effects, and possible courses of action that will help advance the framework of privacy rights to fit the digital age while balancing competing needs: adequate protection for private citizens, and necessary tools and abilities for the government to ensure the safety of its citizens.

Acknowledgements

I would like to thank my primary advisor Professor John Davidson for his incredible insight and genuine interest in a new topic. My discussions with Professor Davidson and the questions he posed were invaluable in expanding my understanding of privacy and challenging my views and conclusions. His guidance was instrumental in shaping this thesis. Additionally, I would like to thank Professor Joan Rocklin for her willingness to take on an advisory role with an undergraduate thesis for the first time. Her knowledge of law and her expertise as a writer were essential throughout this process and I will carry her wisdom with me as I continue beyond school. I am also grateful for the consistent encouragement of Professor Mike Piexoto and for the willingness of Professor Melissa Graboyes to join my panel of advisors very late in the process.

I would like to thank my parents for supporting and encouraging me throughout this process as well as throughout my four years in the Robert D. Clark Honors College. It was through them that I fostered an interest in law and the Constitution. They helped me develop a curiosity in how our foundational legal principles might be adapted to our modern society and encouraged my decision to pursue this interest. Without their unending support and encouragement, I would not be where I am today. Not a day goes by where I fail to be reminded of what incredible role models they are. Mike and Paula Vlaming, I am eternally grateful for you.

Table of Contents

Introduction

Why are Privacy Rights Important?

How important is privacy to the average American citizen? How important is privacy to the function of democracy? What levels of protection can be reasonably expected by those who seek to prevent the unwanted discovery of private information? How do the security interests of the government impact the protection of the American ideals of individualism and privacy? These questions challenge the progress and identity of America. Politicians, legal scholars, civil liberties advocates, and Supreme Court justices all struggle to evaluate these questions and develop adequate answers.

While it is generally understood that privacy is an essential element of modern life, it is difficult to fully describe why it is of such importance and how we should go about ensuring its protection. Privacy is a broad concept that can be concretely described in terms of seclusion and concealment; however, upon a deeper exploration it is clear that it expands beyond simply physical characteristics. The notion of privacy also includes psychological aspects that encompass individuality and personal autonomy, which are grounded in the peace of mind that one is free from unwanted intrusions or disturbances in their personal life, as well as unnecessary limitations and confinements on one's personal liberties. Both of these aspects are essential to the larger idea of privacy, regardless of the situational factors in which they exist. The tangible elements of privacy are crucial to protecting information, while the psychological elements are fundamental to ensuring the independence of the individual. In a

democracy such as the United States of America, each of these aspects of privacy plays a crucial role in facilitating the proper functioning of a representative democracy and the maintenance of our core values.

The right to privacy is not a right that has been specifically outlined in the Constitution or its Amendments; nor has it been a right that has existed with a singular or static definition. It has been exposed to the ever-changing tides of societal norms and technological development, expanding and contracting over decades and shaped by the actions of the Supreme Court and Congress. This progression of the relationship between technology, society, government, and law has been fascinating. However, in recent years, a worrisome gap has developed between the legal framework used to evaluate infringements on individuals' privacy rights and the realities of the societal environment in which this framework is expected to operate. Most judicial precedent and legal theories that have been foundational in the development and evaluation of privacy rights predate the technological advancements that are the source of the current issues revolving around the protection of privacy. Some of these judicial precedents and legal theories have become fundamentally inadequate for their roles in evaluating current issues such as government surveillance and personal data protection. Recently the Supreme Court has faced increasing criticism and skepticism regarding the judicial precedents it has established. Concerned scholars and critics have brought attention to expanding invasions of privacy by government agents and decreased protections for citizens. The growing chorus of fear and distrust has set the stage for another round of landmark Supreme Court decisions.

Privacy Rights: The Foundations and Core Principles

Early Ideas of Privacy

The issues surrounding what have become known as "privacy rights" stretch from their origins in limited legal discussions of the late 1800's, to current national debates of legal rights, technological possibilities, and personal values. Privacy occupies a unique position within American legal history because it lacks the explicit constitutional support that many of our other foundational rights possess. In fact, the word "privacy" never actually appears in the Constitution. Therefore, legal scholars have drawn upon the language of other rights within the Constitution to find "the right to be left alone," which eventually developed into "the right to privacy."[1] This notion of a constitutional right being found in the language of other, more specifically defined rights began in the late 1800s. However, Justice Douglas' majority opinion in the much more recent *Griswold v. Connecticut* (1965) case offers an accurate encapsulation of the "penumbras and emanations" approach that has long been central to the developing notion of privacy rights:

> The foregoing cases suggest that specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance… Various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment, in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner, is another facet of that privacy. The Fourth Amendment explicitly affirms the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The Fifth Amendment, in its Self-Incrimination

[1] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 193

> Clause, enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." [2]

The lack of an explicitly defined right to privacy has allowed for a continuous, if at times inconsistent, development of the notion that individuals have a justifiable interest in protection from unwanted inquiry and discovery of personal information.

The right to privacy is a foundational element of our civil liberties in that it establishes protections intended to shield citizens from excessive government intrusion into their lives and provide citizens with a reasonable expectation that they control access to their personal information. It helps protect the autonomy and individualism that are among the core elements of the American conscience and are essential psychological aspects of democracy. As highlighted by George Orwell's dystopian novel, *1984*, without adequate privacy protections we risk surrendering our psychological and personal autonomy as well as our essential civil liberties at the hands of increasingly complex government control and manipulation efforts. The psychological importance of privacy to the successful function of democracy cannot be ignored; therefore, privacy is implicit in the concept of ordered liberty. As discussed in *McDonald v. Chicago*, a right that is not specifically enumerated in the Constitution can gain constitutional stature if it is believed to be "implicit in the concept of ordered liberty," meaning that it is "essential to free government and to the maintenance of democratic institutions."[3]

---

[2] *Griswold v. Connecticut*, 381 U.S. 484 (1965)
[3] *McDonald v. Chicago,* 561 U.S. 742, 745-747 (2010)

The Fourth Amendment

As reflected in the Fourth Amendment, the most basic tenet of the right to privacy is the Constitutionally guaranteed right of the people to be secure in their "persons, papers, houses, and effects" and to be protected against "unreasonable searches and seizures." When it was written, the Fourth Amendment was designed to primarily protect against physical intrusion by government agents, or other citizens loosely acting as law enforcement officers (which was common at the time).[4] The intrusions that the Fourth Amendment was intended to protect against were those experienced at the time, namely intrusions into one's home or searches through one's personal effects. Physical invasions upon property and possessions were the primary concern long before issues of electronic data collection and surveillance became relevant.[5] To protect against excessive physical intrusions, the framers of the Fourth Amendment stated that such acts were illegal without obtaining a judicial warrant specifically stating the intent, goal, and scope of the proposed search.[6]

The purpose of a warrant is to ensure a check on police power and act as a safeguard against unjust intrusions. It requires police officers and other government agents to give a preliminary description of the search and upon review by an independent judge receive approval of the proposed search.[7] Before approving a warrant request, a detached and neutral magistrate is required to confirm that the

---

[4] Barry Friedman and Orin Kerr, "The Fourth Amendment" *National Constitution Center* https://constitutioncenter.org

[5] "Fourth Amendment: Search and Seizure – History and Scope of the Amendment" *Justia U.S. Law* law.justia.com

[6] "Search Warrants: What They Are and When They're Necessary" *Nolo* http://www.nolo.com

[7] "Warrants" SearchandSeizure.org

requested search is reasonable and that probable cause exists to link the subject of the search to illegal activity.[8] The language of the Fourth Amendment reflects the realities of the threats that existed in 1789 when the it was written.[9] Over time, this language has been liberally construed to include not only protections for the physical confines of one's house, but also protections from intrusions into data, digital communications, and even aspects of one's personal liberty and identity.

[8] "Search Warrants: What They Are and When They're Necessary" *Nolo* http://www.nolo.com
[9] Barry Friedman and Orin Kerr, "The Fourth Amendment" *National Constitution Center* https://constitutioncenter.org

The Progression of Privacy Rights: Development of Doctrines by the United States Supreme Court

Introducing a Liberal Interpretation of the Fourth Amendment

Early common law rights were relatively simple and protected primarily against wrongs committed against a person or his possessions. The closest thing to privacy rights were protections against physical intrusion upon a person's life or his property.[10] Under early understandings of common law, the right to life protected against various forms of physical battery; the right to liberty protected against unjust restraint or imprisonment; and finally the right to property secured a man's control over his land and physical possessions.[11] These basic rights were the same general principles that had been previously established in England dating back centuries; however, as the modern era approached, these principles were expanded upon.[12]

In 1886, the United States Supreme Court authored its first major opinion that included language encouraging the expansion of Fourth Amendment protections with the intent of securing the legitimate interests of "personal security, personal liberty, and personal property" of United States citizens.[13] In the case *Boyd v. United States*, the Supreme Court addressed one of the earliest issues at the foundation of privacy rights. It took on the question of whether or not it was a violation of a defendant's constitutional

---

[10] Daniel J. Solove, "A Brief History of Information Privacy Law" *George Washington School of Law* (See pages 1-11 for an early history of privacy law and an understanding of related common law) (2006)
[11] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 193
[12] See: Albert Kiralfy, Andrew Lewis, Mary Glendon, "Common Law" *Encyclopedia Britannica* (August 5, 2016) https://www.britannica.com/topic/common-law (The definition and description of common law)
[13] *Boyd v. United States*, 116 U.S. 616, 630 (1886)

rights to compel him to comply with a prosecutor's requests that he turn over any private books, documents, or papers under the threat that if he did not comply, all allegations would be assumed as true. The Court decided unanimously that the forced production of a man's private papers amounted to a violation of both his Fourth and Fifth Amendment rights. Justice Bradley concluded that compelling a man to turn over his private papers was essentially the same as conducting a warrantless seizure of the papers and therefore violated his Fourth Amendment right against unwarranted search and seizure. He also argued that forcing a defendant to turn over such papers caused him to effectively become a witness against himself, thus violating his Fifth Amendment right protecting him from forcibly becoming a witness against himself in a court of law.[14]

Justice Bradley understood that this decision would have a lasting impact on the position of the Court regarding Fourth Amendment privacy issues as well as its attitude towards protecting the personal privacies of citizens, and he was therefore particularly intentional with the wording and scope of his argument. He clearly and concisely articulated the core elements of his argument:

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offence, but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offence.[15]

[14] *Boyd v. United States*, 116 U.S. 616, 621 (1886)
[15] *Boyd v. United States*, 116 U.S. 616, 630 (1886)

Justice Bradley's clear view that it is not strictly the breaking down of doors and the rummaging of papers that constitutes a violation of the Fourth Amendment, but rather that it is any form of invasion upon "the privacies of life," meaning an individual's personal security, liberty, or property, is of the utmost importance because it greatly expands the scope of the Fourth Amendment. Declaring the compelled production of personal papers as tantamount to a physical intrusion effectively equates the severity of each offense and consequently recognizes that threats to personal privacy are not limited to physical invasion by government agents. Justice Bradley's opinion helped begin the expansion of the legal understanding of personal privacy as a constitutional right.

The lasting effect of this case was to encourage a liberal interpretation of the Fourth and Fifth Amendments, with the purpose of protecting the right to personal security and personal liberty, as was believed to be intended by the framers of the Fourth Amendment. This precedent is particularly important because it encourages the expansion of the sphere of privacy beyond the limited scope of the protections explicitly stated in the Fourth Amendment. Although it did not affect an immediate and complete shift in the Court's views on the issue, this decision was a key moment for the Supreme Court in that it acknowledged the existence and importance of privacy rights beyond merely the scope of physical intrusion on private residences and conducting searches of papers and files.

Warren and Brandeis: "The Right to be Let Alone"

Four years later, the notion of privacy rights was explored in detail in "The Right to Privacy," an article authored by influential legal scholars Samuel Warren and Louis Brandeis and published in the Harvard Law Review in 1890. In the article, Warren and Brandeis delved deep into the early roots of common law as they built an argument for a right to privacy. Together, they formulated an argument on the basis that the progression of established legal principles and doctrines had broadened to include a "right to be let alone." [16]

Samuel Warren and Louis Brandeis recognized the need to acknowledge and protect a person's spiritual and intellectual being. Gradually the understanding of basic legal principles began to expand to match the increasing sophistication of contemporary societies. Basic rights such as the rights to life, liberty, and property progressively encompassed more than simply the bare minimum required for an individual's survival. The understanding of the right to life expanded to mean the right to enjoy life and slowly incorporated various protections of a person's means of enjoying and fulfilling his ambitions in life.[17] The interpretation of the right to liberty progressed to include civil liberties that protected against much more than unjust imprisonment.[18] The right to property transformed beyond merely a protection of one's land, but also his work and his intellectual property.[19] Warren and Brandeis were instrumental in beginning the expansion of these core tenets of common law, that are at the foundation of our legal

[16] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 193
[17] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 193
[18] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 193
[19] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 193

system, in a way that has encouraged them to evolve alongside the ever-changing demands of our society.

Their concern at the time was the increasingly invasive nature of the press and the media. With the growing use of cameras and the publication of private pictures and stories in newspapers, the authors identified these actions as an invasion of one's personal rights and deserving of legal redress.[20] Warren, in particular, was concerned with the growing means of invading a person's "social privacy," and he felt strongly that there existed a significant community interest in preventing such warrantless invasions upon the private lives of the citizens.[21] They articulated this interest as "the right to be let alone," which protected "the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for rewording or reproducing scenes or sounds" except regarding any matters that may be of a legitimate public interest.[22] Warren and Brandeis argued that this right of the individual to be left alone was substantial and therefore ought to be recognized and enforced by the courts.[23]

Through their unique interpretation and expansion of the existing foundation of tort and common law, which accounted for injuries such as trespass, nuisance, and invasion of privacy, they laid the groundwork of the legal protections of the privacy of individuals. Rather than base the foundation of their concerns in the existing spheres of

[20] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 206
[21] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 214
[22] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 206
[23] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 196-197

contract, libel, property, or trademark law, they argued that it is an individual's more general right to be left alone that protects them from such invasions.

> We must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights as against the world; and, as above stated, the principle which has been applied to protect these rights is in reality not the principle of private property, unless that word be used in an extended and unusual sense. The principle which protects personal writings and any other productions of the intellect of or the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts, and to personal relation, domestic or otherwise. [24]

They favored an expansion of existing privacy protections, such that the new understanding of privacy would acknowledge the rights of the individual and expand the protection of his interests beyond merely those of his physical body or property. Warren and Brandeis' article was the beginning of the development of the right to privacy.[25] Their argument placed privacy rights in the realm of civil tort law, as a protection of the individual against invasions by his peers, rather than a constitutionally grounded restriction against government intrusion. Incorporating the Constitution and applying the right against the government was not the primary goal of Warren and Brandeis' article.

[24] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890) : 213
[25] Dorothy J. Glancy, "The invention of the right to privacy" *Arizona Law Review* vol. 4, no. 1 (1979) : 1

Establishing the Trespass Doctrine: A Property Based Approach

Despite the development of a liberal interpretation of the Fourth Amendment in the *Boyd* decision and the advocacy of the "eternal youth"[26] of common law in "The Right to Privacy," the progression of the right to privacy was not straightforward and at times it even took steps backwards. Forty years later, the Supreme Court again addressed the issue of privacy, this time favoring a conservative view of the law. In the 1928 decision, *Olmstead v. United States*, the Court held that the Fourth Amendment does not protect against warrantless wiretaps placed on phone lines located outside the perimeter of the suspect's private property. The majority opinion reasoned that wiretaps do not physically invade upon the individual's home or his privacy and therefore do not violate his or her constitutional right against unreasonable search and seizure.[27] This decision essentially tied a person's privacy to a particular location, namely their home, establishing physical trespass as the determining factor when evaluating a possible invasion of one's privacy. This subsequently became known as the "trespass doctrine" and guided the progression of privacy rights for decades.

Although the majority decision signaled a shift away from the views expressed in the *Boyd* case and "The Right to Privacy" article, Louis Brandeis, former co-author of "The Right to Privacy" and now a sitting justice on the Supreme Court, used the opportunity to author a highly influential dissenting opinion. In his dissent, Justice Brandeis attacked the *Olmstead* majority's narrow interpretation of the Fourth Amendment and argued that the Amendment's protections should extend to telephone

[26] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* vol. 4, no. 5 (1890) : 193

[27] *Olmstead v. United States,* 277 U.S. 438, 466 (1928)

conversations conducted in private, just as conversations between two people within the confines of a home were protected. His dissent highlighted the changes caused by the incorporation of a new technology, such as telephones, and argued that the rule of law must expand and adapt or risk failing to offer the protections intended by the framers of the Constitution. Justice Brandeis asserted that the protections guaranteed by the Amendment were broader in scope than the literal definition of its language. In his view, the intent of the Fourth Amendment afforded protections beyond merely the physical sense spelled out in the words of the Amendment. In growing with the changing demands of society, it now protected a real and recognizable interest in the psychological wellbeing of the citizenry. He continued to advance the notion of the "right to be let alone," initially expressed in "The Right to Privacy," but in his dissent, he applied it to protecting against government intrusion rather than just intrusion by one's peers.

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of a man's spiritual nature, of his feelings, and of his intellect… They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone - - the most comprehensive of rights, and the right most valued by civilized men.[28]

In this dissent, Justice Brandeis exhibits foresight and reasoning lacked by the other members of the Court. His concern for the rights of the individual, including the psychological aspects of the need for privacy and the need for a fluid relationship

[28] *Olmstead v. United States*, 227 U.S. 438, 478 (1928)

between developing technologies and law helped pioneer views that would become increasingly relevant as the significance of these issues grew.

Establishing the Reasonable Expectation of Privacy Test: Privacy Beyond the Walls of the Home

After the decision in *Olmstead*, the adjudication of Fourth Amendment and privacy rights issues were primarily dictated by the Courts' adherence to the trespass doctrine until the 1960's and 1970's when the Supreme Court began to shift its view. Through several key decisions, the Court departed from its strict reliance on the trespass doctrine and attempted to address concerns that technological and societal advancements were outpacing the law and leaving people unprotected. New doctrines such as the "reasonable expectation of privacy" and the "third-party doctrine" were developed to provide more accurate guidance for the courts when addressing issues of privacy. These changes in legal jurisprudence indicated a more comprehensive approach to privacy by the courts; however, in reality the results were mixed, and in particular situations citizens were still not afforded adequate protection under the law.

The initial departure from the strict use of the trespass doctrine occurred in the case *Katz v. United* States in 1967. Breaking with precedent, the Court held that the Fourth Amendment protects people in situations in which a reasonable person would expect privacy, including situations that take place outside of a private residence.[29] Justice Stewart, writing for the majority, crafted a pivotal opinion. Upending previously accepted logic, he reasoned that the Fourth Amendment's protection of a person's

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

privacy extends beyond a person's physical location within his home and that the trespass doctrine could "no longer be considered controlling."[30] He argued that people can possess a legitimate expectation of privacy, similar to the privacy one has come to expect within one's home, in places outside of their home, and that in such situations, the law must recognize their right to privacy. This argument is significant because, for the first time, the Court detached privacy from specific locations and instead attached it to the reasonable expectations of individuals themselves, regardless of their location.

Thus, the door was opened for the creation of a new legal doctrine that became known as the "reasonable expectation of privacy." The reasonable expectation of privacy is founded on the use of the "reasonable person test." The reasonable person test was first developed as a standard of care to determine liability in cases of negligence.[31] The "reasonable person" for which the test is named is, essentially, a composite representation of a particular community's judgment. It is intended to help evaluate how a "normal" person within in the given community would be expected to behave based on the common views, ideals, and morals of the larger community. It is intended to be flexible and adaptable to changing community standards.[32] This made it particularly appealing for application to privacy law because of its adaptability to changing technological and societal norms. However, this adaptability also makes it vulnerable to significant speculation regarding its legitimacy and effectiveness. The reasonable person test is also inherently susceptible to creating confusion because

---

[30] *Katz v. United States,* 389 U.S. 347, 353 (1967)

[31] See: "The reasonable person" http://legal-dictionary.thefreedictionary.com and "Negligence" http://legal-dictionary.thefreedictionary.com (The definitions and descriptions provided)

[32] Michael W. Price, "Rethinking privacy: Fourth Amendment "papers" and the Third-Party Doctrine" *Journal of National Security Law and Policy* Vol. 8 no. 2 (June 29, 2015) : 262

arguably a person does not know what to "reasonably" expect until the courts give grounds for the expectation, which can only happen once a particular set of events occurs and provides the courts a case on which they can lay the groundwork for the acceptable expectation.[33] In theory the reasonable person test creates a flexible framework in which privacy can adapt to changing technologies and social norms. However, in practice it places a significant burden on the courts to determine what a person may reasonably expect, and whether this is an acceptable expectation for society as a whole.[34] This leads to a problematic application of the doctrine that does not live up to its expectations of flexibility.

In *Katz,* the Court examined whether or not the defendant's rights were violated when government agents placed electronic listening devices on the outside of a phone booth he was known to frequent. The government's argument hinged on two key points: that a phone booth is a public space and therefore it does not enjoy the level of privacy of a house, and second, that even if the phone booth is a protected space, the placement of the listening devices did not constitute an intrusion based on the trespass doctrine because they were located on the outside of the booth and did not physically intrude inside the phone booth.[35] Conversely, the petitioner, Mr. Katz, argued that any reasonable person who engaged in a private phone call within the enclosure of a phone booth reasonably expects that there are no prying ears overhearing the conversation and

[33] See: Michael W. Price, "Rethinking privacy: Fourth Amendment "papers" and the Third-Party Doctrine" *Journal of National Security Law and Policy* Vol. 8 no. 2 (June 29, 2015) (The discussion of the "reasonable expectation of privacy")
[34] Michael W. Price, "Rethinking privacy: Fourth Amendment "papers" and the Third-Party Doctrine" *Journal of National Security Law and Policy* Vol. 8 no. 2 (June 29, 2015) : 261-262
[35] *Katz v. United States,* 389 U.S. 347, 352 (1967)

therefore the use of listening devices intruded upon a situation in which he had a justifiable belief that he was not being overheard.[36]

In his majority opinion, Justice Stewart guided the court to explore a new line of thinking, concluding that the defendant was justified in believing that he had a legitimate expectation that his conversations inside an enclosed phone booth would not be overheard or recorded by any outside persons or devices. He advised the Court to avoid the misplaced emphasis on the notion of a "constitutionally protected area" and the characterization of the phone booth as such.[37] He explained, "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."[38] The Court's decision that the reach of the Fourth Amendment is not directly tied to the occurrence of a physical intrusion into a geographic area, indicated a fundamental shift in the interpretation of the Amendment and resulted in a significant expansion of its protections of personal privacy.[39] As Justice Stewart notes, once this core conceptual shift away from the reliance on geographic areas and physical enclosures is understood, the Fourth Amendment naturally enlarges to protect people based on a situational basis rather than a locational one. Therefore, a person's words may be protected in situations where he or she has a

[36] *Katz v. United States,* 389 U.S. 347, 349-351 (1967)
[37] *Katz v. United States,* 389 U.S. 347, 349-350 (1967)
[38] *Katz v. United States,* 389 U.S. 347, 353 (1967)
[39] See: Nicandro Iannacci, "Katz v United States: The Fourth Amendment adapts to new technology" *National Constitution Center* (December 18, 2015) https://constitutioncenter.org (Discussion of the *Katz v U.S.* decision and the long-term effects of the shift in judicial precedent)

reasonable expectation of privacy, just as his or her private papers within a locked desk were previously protected by the trespass doctrine.

Justice Stewart further expands on this new understanding of the Fourth Amendment by reasoning that an individual could knowingly expose information to the public from the confines of his home and that information would warrant no protection from the Fourth Amendment. Conversely, he explains that an individual may take steps to preserve the privacy of information, even when he is in a public place, and therefore he may have a reasonable expectation that such information is protected by the Constitution.[40] Consequently, the warrantless use of the electronic listening devices to overhear conversations within what are assumed to be the private confines of a publicly used telephone booth constitutes an unreasonable search and seizure, thus violating an individual's Fourth Amendment rights against such intrusions.

Justice Stewart's opinion highlighted the role of technology in the *Katz* case and he embraced the opportunity to advocate for changes in the jurisprudence that would make the Court's opinion relevant to the current society. He advocated for a living interpretation of the Constitution that incorporated changes, such technological developments, into the longstanding protections afforded by the Constitution, in this case specifically the Fourth Amendment. The underlying reasoning being that a living interpretation of the Constitution and the Amendments would ensure that the safeguards intended by the Framers would be maintained, even in an era that was witnessing the development of technologies that were unthinkable in the days of the birth of the Constitution. While examining the issues in the *Katz* case, Justice Stewart noted that the

[40] *Katz v. United States,* 389 U.S. 347, 351 (1967)

Court could not ignore the fact that the telephone had become an integral part of people's lives and, therefore, its role in daily life deserved to be considered when interpreting the scope of the protections of the Fourth Amendment. He defends his position saying,

> A person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, 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. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[41]

Privacy advocates continue to support this argument, arguing that interpreting the Constitution in a narrow manner, one which ignores the realities of technological development and the resulting societal changes, is to ensure the failure of its intended protections. The views that Justice Stewart expressed in his *Katz* opinion were pivotal in shifting the direction of privacy jurisprudence and succeeded in expanding the legal understanding of privacy rights beyond the earlier property based boundaries.

Establishing the Third-Party Doctrine: External Actors

Shortly after the introduction of the reasonable expectation test to Fourth Amendment jurisprudence, the Supreme Court developed another doctrine, this one specifically for privacy rights. The Court heard several cases that addressed the accessibility of information and the legal protections that existed for individuals seeking to maintain the privacy of their personal information. Through these cases, the Court

[41] *Katz v. United States,* 389 U.S. 347, 352 (1967)

developed the third-party doctrine, which became one of the primary guiding principles of privacy law, alongside the reasonable expectation of privacy test.

The third-party doctrine loosely relies upon the reasonable expectation test in that it helps evaluate situations in which a person may reasonably expect to control the privacy of their information.[42] The third-party doctrine provides that if a person voluntarily shares information with a third-party, then the individual no longer has any legal grounds to expect to maintain the privacy of the information that was shared.[43] It created a bright line test which provides constitutional protection for information that is never shared with a third-party, but removes any protection or warrant requirement for information that is disclosed to any other person or institution, regardless of the nature of the third-party or the purpose that the party serves in acquiring or transmitting the information. This standard means that government agents such as the FBI or the police can access information in many situations without needing a warrant.

One of the first cases introducing the third-party doctrine was *California Bankers Association v. Shultz,* decided in 1974. In *California Bankers Association,* the Supreme Court addressed issues regarding the Bank Secrecy Act of 1970. The Act required detailed record keeping of depositors' financial records as well as compulsory production of such records upon request by government agents.[44] In terms of privacy rights, the question was whether an individual could maintain a reasonable expectation of privacy over personal information that had been shared with an institution such as a

[42] Michael W. Price, "Rethinking privacy: Fourth Amendment "papers" and the Third-Party Doctrine" *Journal of National Security Law and Policy* Vol. 8 no. 2 (June 29, 2015) : 262
[43] John Villasenor, "What You Need To Know About The Third-Party Doctrine" *The Atlantic* (December 30, 2013) https://www.theatlantic.com
[44] *California Bankers Association v. Shultz,* 416 U.S. 21, 21-22 (1974)

bank. The case was framed in such a way that it resembled the earlier *Boyd* case in that the government sought the compelled production of papers in hopes of proving a financial crime. However, unlike in *Boyd,* where the defendant was in possession of the papers, in *California Bankers Association,* the bank was in possession of the desired records. This then raised the question of whether the defendant's Fourth and Fifth Amendment protections, the same protections that were affirmed in the *Boyd* decision, extended to personal information that was in the possession of the bank.

The Supreme Court's opinion in *California Bankers Association v. Shultz* held that the personal privacy interests protected by the Fourth and Fifth Amendments do not extend to institutions such as banks, and therefore the government can compel even unwilling banks to turn over their records upon request, for the purpose of investigating criminal tax and regulatory activities, without violating citizens' privacy interests. The Court determined that the Bank Secrecy Act does not violate the Fourth Amendment search and seizure clause because the government can access the records only through existing legal processes and is not conducting an unreasonable intrusion because the records are held by a third-party rather than the depositors themselves. The Court also held that it does not violate the banks' Fifth Amendment right against self-incrimination because, as a corporation, banks do not have that right which is strictly reserved for people. This decision determined that the provisions of the Act did not violate the depositors' Fifth Amendment right against self-incrimination because the evidence would be produced by a third-party who has no interest against self-incrimination.

Justice Thurgood Marshall recognized the challenges posed by the adoption of the third-party doctrine and authored a compelling dissent in *California Bankers'*

Association. His dissenting opinion returned to the logic of the *Boyd* decision and condemned the majority opinion for being "wooden" and ignoring both the fact that current technological developments make brute force searches and seizures all but obsolete, as well as the precedents established in *Boyd* and *Katz*.[45] He argued that the provisions of the Bank Secrecy Act were tantamount to a search and seizure under the Fourth Amendment for several reasons. His primary grievance was with the notion that individuals inherently forfeit their interest in the privacy of their information by disclosing it to a bank for a narrowly defined purpose within the confidential consumer-bank relationship.[46] He also disagreed with the majority on the grounds that their decision essentially allowed the government to bifurcate the banks' record keeping process and the government's inquisition process in such a way that effectively eliminated any privacy interests of the depositors.[47] Justice Marshall contended that the Court had allowed the government to use the third-party doctrine to create a loophole through which it could easily access the personal financial information of citizens. The government created this loophole by enacting legislation requiring banks to fulfill the preliminary steps of gathering and recording the financial information of its clients, and then later compelling the banks to turn over the records against their will on the grounds that the information recorded by the banks had been cleansed of any of the depositors' Fourth Amendment interests by the fact that the information was in the possession of a third-party. In summation, Justice Marshall asserted that the Court's decision had used

[45] *California Bankers Association v. Shultz*, 416 U.S. 21, 95 (1974)
[46] *California Bankers Association v. Shultz*, 416 U.S. 21, 95-96 (1974)
[47] *California Bankers Association v. Shultz*, 416 U.S. 21, 96 (1974)

legislation in conjunction with the third-party doctrine to unfairly strip the depositors of their Fourth Amendment rights.

Justice Marshall's dissent in the *California Bankers Association* case is the first to highlight what will eventually reveal itself as a fundamental fault line in the current jurisprudence of the Fourth Amendment and privacy rights. The continued use of the third-party doctrine highlights the glaring inadequacy in the modern application of a dated doctrine. When broad exceptions to the protections of the law are made in instances such as this, more than just criminals are affected; all citizens become subject to government intrusion and the loss of fundamental privacy rights that are essential to their psychological and emotional wellbeing, as well as their identities as autonomous individuals engaged in the social and democratic networks of this country.[48] This doctrine was adopted to help the courts arrive at consistent decisions when evaluating claims of Fourth Amendment protection, but it has significant implications, erasing the boundaries that protect the public from government intrusion.

Justice Douglas also disagreed with the decision of the Court and offered another dissenting opinion that rings true decades later. Decades removed from this particular decision, his concerns have only increased in relevance today. He took a direct stand against the government's claim that the collection of every citizen's bank records was a necessary and effective means of investigating crime.[49] In his view, the indiscriminate collection of every private citizen's information was a gross overreach of

[48] See, Woodrow Hartzog and Evan Selinger, "Obscurity: A better way to think about your data than 'privacy.'" *The Atlantic* (January 7, 2013) https://www.theatlantic.com and Julie E. Cohen, "What is privacy for" *The Harvard Law Review*, no. 126 (November 5, 2012). Role of privacy as essential to personal autonomy, personal identity, as well as social and political participation.
[49] *California Bankers Association v. Shultz,* 416 U.S. 21, 85-86 (1974)

government power and he denounced the program as "unadulterated nonsense unless we are to assume that every citizen is a crook, an assumption I cannot make."[50] He aptly describes the government's plan of mass record collection as a "sledge-hammer approach to a problem that only a delicate scalpel can manage."[51] Although Justice Douglas' language was referring to the collection of bank records such as checks, it is almost directly applicable to the mass surveillance and metadata collection programs the government uses today. These programs also treat all citizens as if they were crooks and gathers their data without any prior suspicion of a crime, mirroring Douglas' earlier fear of a "sledge-hammer approach." This was a dangerous precedent to set and it is clearly continuing today in the form of even more intrusive programs.

Later cases developing the third-party doctrine include *Smith v. Maryland* and *United States v. Miller*. In *Smith v. Maryland*, decided in 1979, the Court further supported the third-party doctrine as the defining doctrine underlying privacy rights. In its decision, the Court said, "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[52] The language in the *United States v. Miller* decision is even more troubling. The Court held that,

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third-party and conveyed by him to Government authorities, even if the information is revealed on the

[50] *California Bankers Association v. Shultz*, 416 U.S. 21, 85 (1974)
[51] *California Bankers Association v. Shultz*, 416 U.S. 21, 85 (1974)
[52] *Smith v. Maryland*, 442 U.S. 735, 743-744 (1979)

> assumption that it will be used only for a limited purpose and the confidence placed in the third-party will not be betrayed.[53]

This solidified a problematic precedent, effectively determining that individuals should have no confidence in any information they might be required to release to a third-party, even for limited and defined purposes.

Using the Established Doctrines in Conjunction with Each Other

After establishing the reasonable expectation test and the third-party doctrine as the prevailing legal tradition in terms of settling privacy disputes, the Court was presented with privacy issues arising at the intersection of the two doctrines. The issue in *Smith v. Maryland (1979)* was whether or not the warrantless use of an electronic pen register to record the numbers dialed by a telephone constituted a violation of the dialer's reasonable expectation of privacy. [54] The pen registers were installed at the central offices of the telephone company at the request of police officers. Therefore, the pen registers were recording data, in the form of the dialed phone numbers, that had been intentionally sent to the phone company by the person dialing the phone. Hence, the decision hinged on the two interconnected legal doctrines. First, does the telephone company qualify as a third-party, and therefore, does any information transmitted to it lose any Fourth Amendment protections? And secondly, does a telephone user possess a realistic claim to a "legitimate expectation of privacy" regarding the numbers he dialed into his phone? [55]

---

[53] *United States v. Miller*, 425 U.S. 435, 443 (1976)
[54] *Smith v. Maryland,* 442 U.S. 735, 736 (1979)
[55] *Smith v. Maryland,* 442 U.S. 735, 735 (1979)

The Supreme Court decided against the petitioner, determining that the Fourth Amendment protects an individual only if the individual justifiably believes that the government has invaded his or her reasonable expectation of privacy. The majority of the Court believed that since the users of telephones regularly and voluntarily transmit the phone numbers they dial to the phone companies in the course of conducting their regular business, they have no reasonable expectation that those particular numbers are protected by the Fourth Amendment and are exempt from being shared. The justices concluded that users of telephones knowingly convey personal information to institutions, that the users know said institutions have the capability to record such information, and therefore the users assume the risk that said information could potentially be divulged to police.[56]

As with *California Bankers Association*, Justice Marshall again disagreed with the majority's opinion for several reasons. First, he took issue with the majority's assumption that most individuals "typically know"[57] that a phone company monitors and records the telephone numbers dialed for business purposes. He argued that it is unreasonable to assume that the majority of people operate with that conscious understanding.[58] Second, he argued that the individual's choice to voluntarily turn over that information in the course of conducting regular business with the phone company, if no reasonable or practical alternative exists, is not a valid reason to believe that the individual willingly forsook their interest in maintaining the privacy of that

[56] *Smith v. Maryland*, 442 U.S. 735, 745 (1979)
[57] *Smith v. Maryland*, 442 U.S. 735, 749 (1979)
[58] *Smith v. Maryland*, 442 U.S. 735, 749 (1979)

information.[59] This aspect of his argument rests on the notion that simply transmitting information to such institutions as a bank or phone company for limited business purposes is essential to normal daily function in modern society, and it does not automatically mean that one intended to accept the risk that said information would be released to other people, including the government.

The logic of the majority opinion has proven to be substantially damaging to the real-world privacy expectations of citizens. In *Smith,* the majority articulated a two part reasoning: first, that information transmitted to an institution, such as a telephone company, for a limited purpose within the defined role of an essential function of modern society is not within Fourth Amendment protections; and second, that individuals generally understand when and where they are voluntarily transmitting personal information to a third-party that is not legally bound to preserve the secrecy of that information, and therefore cannot reasonably expect that privacy to be maintained.

The precedent established in *Smith* and in *Shultz* indicates the Court's belief that individuals ought to have a minimal or even nonexistent expectation of the privacy regarding personal information such as their phone records and financial records, despite the fact that there are few alternatives for individuals who wish to maintain the secrecy of such information. Seamlessly engaging with institutions such as banks and phone companies has become an essential part of our integrated society, and as a result there are very few alternatives for individuals who want to keep their information out of the hands of these third-party institutions. The issue of shared information has been compounded by the fact that institutions such as banks and cellular providers have

[59] *Smith v. Maryland*, 442 U.S. 735, 750 (1979)

collected increasing amounts of information that create the increasing possibility of developing a clear understanding of the personal aspects of their customers lives. In addition, the few alternatives that exist, such as strictly completing monetary transactions with cash or placing calls using only a prepaid phone that does not correlate to any personal records, are highly inefficient and often significantly more costly than the mainstream alternatives. This lack of realistic alternatives for conducting daily business in ways that ensure the secrecy of personal information is a substantial barrier to the realization of our rights against unreasonable search and seizure. It effectively acts as a loophole that ensures that much of our personal information is available for government access, under the illusion that a voluntary choice was made to relinquish the constitutional protections.

New Advances in Technology Create Problematic Privacy Scenarios

Technological Advances and the Related Issues

Over time, technology has advanced and new developments have become incorporated into our daily lives, dramatically changing the ways in which we share, store, and discover information. Advances in the capabilities of the Internet, personal computing devices, and global positioning systems (GPS) are some of the most dramatic examples. Today's most advanced cellular phones are capable of monitoring location, storing photos and videos, and supporting countless social media platforms through which we share details of our lives and indicate our interests, social and political preferences, and hobbies. Cellphones are also capable of recording our contacts and all the information shared with them such as text messages, emails, and transcripts of phone calls. This wealth of information is not only stored on the cell phone itself, it is also recorded by external entities such as cellular and internet service providers, and in digital spaces such as the "cloud." In addition to the data collected by cell phones, records are also kept of all browsing and shopping activity conducted on the Internet.[60] Whether it is recorded for advertising purposes or simply through the process of conducting business, this information is compiled and monitored by a third-party, often the cellular service providers or the internet service providers. Seemingly insignificant information such as Internet browser history or date and time records of calls and texts

[60] Olivia Solon, "Your browsing history may be up for sale soon. Here's what you need to know" *The Guardian* (March 28, 2017) https://www.theguardian.com

can reveal very intimate and personal details that an individual has no intention of sharing.[61]

The increasing capabilities of tools for information gathering and sharing, driven by technological advancements, have ensured a corresponding increase in the ways to intrude upon one's privacy. These new forms of creating and managing information have given rise to a complicated network of players in the world of information services, each one independently collecting and distributing data, thus making it increasingly difficult to maintain privacy protections.[62] As a result of these technological advances, invasions of privacy are no longer limited to the brutish methods of entering a home and searching through papers. Today there are far more covert ways for people, both government agents as well as private corporations, to search through the personal details of private citizens' lives and acquire knowledge of their private affairs. For example, Internet service providers (also known as ISPs) are able to track Internet browsing patterns which often reveal information such as personal health concerns, religious views, banking and shopping patterns, political affiliations, and even sexual orientation.[63] This information is usually collected under the guise of advertising purposes, but sensitive personal information such as this can be used in much more malicious ways depending on who possesses it and how they intend to use it. For example, personal information can be used to develop targeted political

---

[61] Tom Wheeler, "Protecting Privacy for Broadband Consumers" *Federal Communications Commission* (October 6, 2016) https://www.fcc.gov

[62] Olivia Solon, "Your browsing history may be up for sale soon. Here's what you need to know" *The Guardian* (March 28, 2017) https://www.theguardian.com

[63] Olivia Solon, "Your browsing history may be up for sale soon. Here's what you need to know" *The Guardian* (March 28, 2017) https://www.theguardian.com

messaging strategies which can ultimately affect politics on the national level.[64] Additionally, even if one's personal information is not being gathered with harmful intentions, it is still disconcerting to have the details of one's life so readily accessible by unknown individuals.

For all their benefits in increasing efficiency and productivity, bringing unprecedented knowledge and power to our fingertips, and providing platforms for people to connect in new and innovative ways, the Internet and other technological advancements have arguably led to an effective decline in the privacy of individuals. The development of new ways for private citizens to communicate, store, and discover information and data have opened the doors for unforeseen means of government intrusion and surveillance. Information that previously would have been considered private is much more likely to be assumed as public in the current digital and social environment. New technologies have eased the means of discovering information that once would have been impossible to know without a clear violation of one's rights. Technology has blurred what was once a clear line between public and private, and as a result citizens no longer enjoy the same level of privacy that they once did.

The incorporation of new technologies into our lives has dramatically restructured the underlying foundations of our society, forging a now global community and connecting people in entirely new ways that encourage unprecedented levels of information sharing. The rise of social media has encouraged the voluntary disclosure

[64] See e.g.: Tom McCarthy, "How Russia used social media to divide Americans" *The Guardian* https://www.theguardian.com (October 14, 2017) (The discussion of how Russia used targeted messaging tactics to divide Americans along lines of race, religion, class, and creed to influence the 2016 presidential election.)

of life events, personal interests and activities, and political views. As people's online presence grows, there is a corresponding decrease in expectations of an expectation of privacy. The more we share with the world, the less we expect to remain private. These changes in social behavior have created a problematic shift in the *expectation* of privacy by encouraging people to voluntarily relinquish their privacy without concern for the consequences. It is increasingly difficult to maintain a legal expectation of privacy in an environment where personal information is voluntarily made public.

We live in an environment where the privacy of information is no longer guaranteed by the simple measures of a locked desk drawer or the confines of a private residence. The incorporation of technology into our daily lives has progressed to the extent that as members of modern society, it is impossible to conduct our daily business without using digital devices to some extent. Even without voluntarily sharing personal information on social media sites, using common devices such as cell phones, laptops, and credit cards comes at the price of leaving behind a detailed account of our personal lives that can be traced by the institutions that facilitate these services.

The simple fact that all this information can be condensed onto a single device such as a personal computer or a cell phone, devices that are constantly recording and transmitting information as well as perpetually monitored by cellular networks and Internet service providers, presents enormous challenges with regard to maintaining the privacy of information. This effectively removes personal information from the physical control of the individual to whom it pertains; instead, placing it under the control of third parties such as corporations, who have very different legal obligations and protections than people. An environment such as this requires a legal and legislative

approach that relies less on the physical location and control of information and more on a comprehensive content based approach. These new developments in the transmission and storage of information expose the substantial differences between the law and the reality in which we operate today, differences that threaten the privacy of private citizens.

The digital age and the ever-expanding technological capabilities of modern society have created the frightening possibility of government agents accessing all the intimate and personal information stored on a cell phone or computer; however, scary headlines like these often overlook the equally troubling aspects of more covert and passive methods of data collection. Access to a large enough sample size of simple data records, such as phone logs, purchase and search histories, and locational data points, can give police officers a detailed summary of personal aspects of life that can be just as revealing as actively personal notes, emails, or text messages. In previous decades, such information would have been considered impossible to know without the help of massive amounts of time and resources. Now, this information is easily compiled and accessible by government agencies thanks to advances in computing technology and cooperation with private sector companies such as Verizon, Apple, Facebook, Google, and Yahoo.[65] In recent years, concerns regarding government surveillance of this type of data has made headlines, but there has been little judicial progress made in updating the guidelines regulating protections of this information.

[65] Timothy B. Lee, "Here's everything we know about PRISM to date" *The Washington Post* (June 12, 2013) https://www.washingtonpost.com

When exploring this particular relationship between technology, society, and law, it is important to keep in mind the ways in which they affect each other. Technological advances are often incorporated into society far before legislatures and courts have a chance to review and evaluate these changes. Therefore, the courts are repeatedly in the position of reacting to the issues that arise as a result of these changes. As we are seeing in the most recent cases, the courts are being forced to apply legal precedents that were developed long before the modern digital era to issues that are a direct result of the astonishingly rapid and complex growth of digital technology.

Sensory Enhancing Technology

In addition to the narrowing scope of privacy protections, technological advancements have compounded the threat to privacy rights by enhancing the methods of conducting searches and increasing law enforcement officers' ability to discover information without engaging in traditional investigative methods. Interestingly, these technological advances have ignited a revival of the debate of the trespass doctrine. There are a growing number of instances in which the once clear boundaries afforded by the trespass doctrine have been blurred or negated by the use of new technologies. New technological advancements have given law enforcement agencies the ability to intrude on private spaces without physically trespassing. In the current environment, it is harder than ever to define and protect private property even though that has long been considered the most straightforward of privacy issues.

In the 2001 case *Kyllo v. United States*, the police used a thermal imager to detect unique heat signatures in the home of a suspected marijuana grower. Using the

thermal imager, the police identified hot areas on the exterior of the house that would suggest the use of high intensity lamps necessary for growing marijuana plants indoors. Based on this information, the police were able to obtain a search warrant to search the home, where they subsequently found marijuana plants and arrested the owner. [66]

The use of a thermal imager meant that the police could gain an understanding of the physical nature of the interior of the home without ever intruding on its physical premises or revealing any intimate details of the suspect's life, thus, arguably avoiding any invasion that would constitute a violation under the Fourth Amendment. The police also argued that the thermal imager ought to be considered a simple sensory enhancer, and that, since the use of tools such as binoculars and flashlights were not deemed unreasonable, neither should the use of the thermal imager be so deemed.

However, the Supreme Court held that the use of the thermal imager did amount to a Fourth Amendment "search" because the government used a device that is not in "general public use, to explore details of a private home that would previously have been unknowable without physical intrusion."[67] Justice Scalia, who authored the majority opinion, approached the issue with an originalist perspective[68] and presented an argument in favor of acknowledging the original intentions of the Fourth Amendment and protecting these fundamental interests against future erosion by the use of new technologies by the police. Justice Scalia's opinion offers strong support for the

[66] *Kyllo v. United States,* 533 U.S. 27, 27-28 (2001)
[67] *Kyllo v. United States,* 533 U.S. 27, 27 (2001)
[68] See e.g. In a Political Science course at the University of Oregon titled "U.S. Supreme Court," taught by Professor Allison Gash, we examined various interpretations of law and some of the justices that adhered to each interpretation. This included originalism and we studied Justice Scalia as one of its primary advocates. Specific decisions we studied were: *Lawrence v Texas, District of Columbia v Heller,* and *Planned Parenthood v Casey.*

protection of the privacy of the home. Using the logic applied in *Katz*, which declared that an eavesdropping device that picks up the sound waves leaving the enclosure of a phone booth is tantamount to a search and is therefore a violation of the Fourth Amendment, Justice Scalia arrived at the conclusion that a thermal imager used to detect the heat waves emanating from a house must also constitute a violation of the Fourth Amendment. It is ironic, however, that he invokes the reasoning used in *Katz* to argue in favor of a continuation of the trespass doctrine, when *Katz* was in fact the decision where the Court first implemented the reasonable expectation test and intentionally departed from a strict reliance on the trespass doctrine. Scalia argues that to declare otherwise would "leave the homeowner at the mercy of advancing technology-including imaging technology that could discern all human activity in the home."[69] While ironic that Justice Scalia would formulate his argument in such a way, he does make an important point in acknowledging the importance of advancing the interpretation of the Fourth Amendment to maintain the relevance of its protections in the face of advancing technology.

Changes in Investigatory Strategies and Capabilities

As technology has progressed, the government continues to utilize new methods of acquiring data that records the details of our personal lives. In addition to simply providing new tools and instruments with which information can be accessed or discovered, new technology can also compile and analyze unprecedented quantities of

[69] *Kyllo v. United States,* 533 U.S. 27, 28 (2001)

data. These new advancements have removed the physical and resource barriers that used to prevent government agents from pursuing certain types of surveillance.[70] The fundamental limitations of finite resources and man-power formerly ensured constraints on the government's ability to track the private information of citizens. For example, the police could theoretically manually comb through countless phone records, financial transactions, and surveillance camera tapes to establish an understanding of the details of a person's life, but due to the realistic limitations of available resources it was naturally assumed that this was impossible and there was little value in such information because it came in such large data sets that it was a fruitless task to attempt to make sense of it. However, technological advancements have exponentially increased the efficiency of these tasks and, therefore, enable government agents to record and analyze unprecedented amounts of data. Government agents can now gain insight into meaningful details of our lives from simple data records that may not necessarily contain any meaningful information in isolation, but when combined with thousands or millions of other data points, can create a thorough picture of one's life.[71]

Issues pertaining to police use of technology and the role technological developments have played in altering the way the police conduct investigations into the lives of suspects have been increasingly scrutinized in court cases. In 2012 the Supreme Court issued a decision on a case questioning the constitutionality of the warrantless use of a GPS tracking device to monitor the movements of a suspect. In *United States v.*

[70] Woodrow Hartzog and Evan Selinger, "Obscurity: A better way to think about your data than 'privacy.'" *The Atlantic* (January 7, 2013) https://www.theatlantic.com
[71] Anthony Barkow, "Symposium: A whole lot of *Wurie*: Information acquisition and the Fourth Amendment" *SCOTUSblog* (June 26, 2014) http://www.scotusblog.com

Jones, police attached a tracking device to the car of a suspected drug dealer without first obtaining a warrant and tracked his location for a month before arresting him on charges of drug possession.[72] In light of these facts, the Court had to directly address the use of GPS devices in relation to the privacy of individuals. Ultimately the Court ruled that the warrantless use of a tracking device constituted an unlawful search and violated the suspect's right to privacy by usurping his property for the purpose of gaining insight to his location.[73]

United States v. Jones highlights the way that technology has changed investigative strategies and the new ways that insight can be gained into the private details of individuals' lives. The suspect, Jones, was driving his vehicle on public roads and in full view of the public, so theoretically it may have been possible for a police officer to follow Jones and learn the same information that was transmitted by the GPS tracking device. Clearly, this tactic would be inefficient and made exponentially easier with the use of a tracking device, thus raising the important question of whether or not it is permissible for law enforcement officers to use electronic devices to gain information that could have theoretically been gained through other means, even though those other means are so highly inefficient as to be effectively impossible.

The Supreme Court determined this to be a violation of Jones' rights; however, members of the Court disagreed with regard to the reason why. The majority opinion was grounded in the belief that the use of an electronic tracking device on his personal vehicle amounted to a trespass on his property. Their reasoning offered a very narrow

[72] *United States v. Jones,* 565 U.S. 945 (2012)
[73] *United States v. Jones*, 565 U.S. 945 (2012)

decision that was strictly limited to the facts of the case and did not offer a broader line of reasoning that would indicate a change in the existing jurisprudence. Their decision effectively relied on the old trespass doctrine and ignored the opportunity to adapt Fourth Amendment interpretation to the norms of the 21st century in any scope beyond the most minimally necessary of steps.

Justice Sotomayor and Justice Alito concurred with the majority; however, they disagreed with the emphasis on trespass doctrine because they believed this line of reasoning constrained the interpretationbg of the Fourth Amendment. Instead, they believed that the decision turned on the notion that the use of a tracking device violated Jones' reasonable expectation of privacy.[74] This distinction in reasoning is important because it demonstrates Justice Sotomayor's and Justice Alito's belief in a broader interpretation of the Fourth Amendment and the protection of a larger sphere of privacy grounded in a person's "reasonable expectation of privacy," rather than simply a property-based approach. The concurring opinions of Justices Sotomayor and Alito offer encouragement that some justices are supportive of a more substantive shift in jurisprudence and that the issue may be revisited sometime in the near future. Their opinions encouraging the broader protections of an individual's "reasonable expectation of privacy" may very well lay the groundwork for pivotal future decisions, just as the dissenting opinions of Justices Brandeis and Butler in *Olmstead* laid the foundation for the majority opinion in *Katz.*

[74] *United States v. Jones,* 565 U.S. 147,155 (2012)

Changing Norms and Altering Police Practices

Technological advancements have encouraged new norms and practices that create a challenging environment for privacy. Practices such as consolidating important information into centralized and accessible means of storage such as in portable devices like cell phones and laptops or in digital spaces such as the 'cloud' mean that vast amounts of information are accessible at once. Information that once would have been distributed amongst any number of notes, files, books, offices, and homes can now be contained within a device that is in our pocket at all times. The police certainly may not access these devices at will; however, the information is neatly consolidated in one place and the law has had to adapt to account for this. It is essential that the law does not maintain a reliance on old understandings of privacy, and instead acknowledges the new ways that information may be accessed and privacy infringed upon.

In 2014, the Court ruled on *Riley v. California,* a case which recognized the importance of cell phones and whether they deserve a higher standard of privacy based on the wealth of information potentially stored within them. The case addressed the ways in which cell phones might change the longstanding rule that allowed police officers to conduct a search of items found on a person's body and within their immediate control during an arrest. The facts of the *Riley* case state that the police arrested David Riley in connection with possession of contraband and firearms that were discovered in the car he was driving. During the arrest, officers looked through images stored on a cell phone that was located in Riley's pocket. A gang specialist used the photos and videos on the phone to determine that Riley was affiliated with a gang. Based on the images as well as ballistics tests from the firearms, Riley was charged in

connection with an earlier shooting incident. Before trial, Riley attempted to suppress the evidence regarding his gang affiliation on the grounds that it was based on evidence that was illegally obtained from his phone during his arrest and without a warrant. His motion was denied and he was convicted but was able to appeal all the way to the Supreme Court.[75]

Riley addresses an important privacy issue with regard to the integration of cell phones into our daily lives and the limitations of search and seizure abilities of law enforcement officers. Previous case law stipulated that law enforcement officers may conduct a warrantless search of items on the body and within the immediate control of individuals during an arrest for the purposes of maintaining officer safety and preserving evidence.[76] The officers reasoned that their search of Riley's cell phone fell within the parameters of maintaining safety and preserving evidence. The Court, however, ruled in favor of Riley, stating that searching the digital data of a cell phone before obtaining a warrant satisfied neither the safety nor the preservation prerequisites and therefore violated Riley's privacy. Perhaps most importantly, the Court distinguished cell phones from wallets and other items that are traditionally found in the pockets of arrestees because they are essentially minicomputers and contain unparalleled amounts of personal information.[77] The Court recognized both the integration of cell phones into daily life, as well as their vastly different nature from

[75] *Riley v. California,* 573 U.S. 1 (2014)
[76] *Chimel v. California,* 395 U.S. 752, 763-763 (1969)
[77] See: "Fourth Amendment: Warrantless Searches Incident to Arrest" *Legal Information Institute* https://www.law.cornell.edu (Explanation of what personal items are usually subject to search incident to arrest, allowing for a better understanding of the distinction the Court was making in the *Riley* decision)

other personal items that may be found on a person during an arrest, due to their content storage capabilities. Acknowledging the importance of maintaining the privacy of devices that contain the most intimate details of our lives is a significant advancement of Fourth Amendment privacy rights by the court.[78]

Although the *Riley* case produced an encouraging decision that indicates an evolving perspective by the Supreme Court, it was again a narrow decision and included exceptions to the warrant requirement in instances of an emergency. Like the *Jones* case, the Court failed to make full use of an opportunity to adequately advance privacy rights into the digital age and ensure the necessary protections for personal digital information. This partially reflects the incremental nature of the Court's jurisprudence, but it also demonstrates a level of hesitancy and uncertainty with regard to the future of this particular area of law. As we have seen, it is changing at an incredibly rapid pace, and, as a result, it is difficult for the courts to anticipate and respond as needed. I believe that these recent decisions indicate a slowly increasing willingness of the Court to address the relevant issues involving technology and the role it plays in privacy. I also believe that the Court will need to issue more comprehensive decisions in the future, decisions that address the broader scope off privacy issues rather than the narrowest meaning of each set of facts if it is to keep privacy from being permanently crippled or destroyed entirely.

Turning an eye towards the near future, the Supreme Court is set to hear a case during its fall 2017 session that has the potential to dramatically change the privacy law landscape. *Carpenter v. U.S.* addresses the significance of cell phone location history

[78] *Riley v. California,* 573 U.S. 9 (2014)

and the constitutionality of government access to this information through third-party cellular providers. The facts of *Carpenter* state that in 2011, police arrested four men in connection with a string of armed robberies. After the arrests, the FBI applied for orders from judges to obtain "transactional records" of the cell phones of each of the men arrested. Using the guidelines of the Stored Communications Act, the judges granted the orders and compelled the cellular providers to turn over records for each of the phone numbers.

The Stored Communications Act dictates that if the government can use "specific and articulable facts [to] show that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation" then it can require that providers disclose particular telecommunication records.[79] Notably, the Stored Communications Act merely requires the officers demonstrate "reasonable suspicion" in order to gain access to the cellular records, rather than the more rigorous standard of "probable cause" that is required when applying for a warrant.[80] The records spanned a 127-day period, including information such as the date and time of calls, the other cellular numbers involved in the calls, and the locational cell site information based on communication with cell towers in close proximity to the phone. The

[79] See: "Carpenter v. United States." *Oyez,* (September 5, 2017) www.oyez.org/cases/2017/16-402. (Provides a concise and effective synopsis of the case and its surrounding issues)
[80] Orin Kerr, "Supreme Court agrees to hear 'Carpenter v. United States,' the Fourth Amendment historical cell-site case" *The Washington Post* (June 5, 2017) https://www.washingtonpost.com

locational records showed that the suspected robbers' cell phones were within a half-mile to two-mile range of the robberies at the times they were committed.[81]

During the court proceedings, one of the defendants, Carpenter, moved to suppress the cell-site evidence on the grounds that the FBI should have needed to demonstrate probable cause and obtain a warrant in order to access his cellphone records. Thus, the primary issue of the case turns on the question of what level of privacy do cell phone records deserve? Because these records are simply non-content metadata and not actual content data, do police need to simply demonstrate "reasonable suspicion" in order to gain access? Or does this metadata deserve a higher level of privacy protection, similar to that of content data, because of the relatively new ability to compile a thorough and accurate picture of one's life based on these data points? If we are to believe that metadata such as time, duration, recipient, and location points can convey a similar level of intimate personal knowledge as the content of the call itself, then the answer to the latter question is 'yes,' and it is imperative that it is protected by the Fourth Amendment and the requirement of a warrant.

While it is clear that *Carpenter* presents the Supreme Court with an opportunity to address significant issues such as distinguishing the privacy interests of metadata and content data, changing the guidelines of the third-party doctrine, and determining how the Fourth Amendment applies in a world of mass surveillance, it is unclear what the Court will make of this opportunity. There has been expressed interest, by Justice Sotomayor in particular, in revisiting and revising the third-party doctrine, which offers

[81] Orin Kerr, "Supreme Court agrees to hear 'Carpenter v. United States,' the Fourth Amendment historical cell-site case" *The Washington Post* (June 5, 2017) https://www.washingtonpost.com

an encouraging outlook for the potential for significant headway to be made in this decision. However, this optimism is curbed by the recent appointment of Neil Gorsuch to the Court, ensuring the maintenance of a conservative-leaning balance of Justices. *Carpenter v. U.S.* promises to provide the opportunity for a landmark decision in the realm of privacy rights, potentially advancing privacy jurisprudence in a way that makes its guidelines more applicable to modern standards and increasing protections of technological aspects of individuals' privacy.

Current Issues: Why are Privacy Protections Fundamentally Flawed Today?

Balancing Security and Privacy: Surveillance and Privacy in The Post 9/11 World

The foremost issue currently dominating the discussion of privacy rights in the digital age is the ultimate need to ensure the safety and security of the United States. The duty of the government to protect the country from threats both foreign and domestic has become increasingly difficult, and as a result, government agencies have implemented practices such as mass surveillance. These types of technologies and programs are new and relatively unproven, leading to fierce debate over whether or not they should be sustained. A troubling lack of transparency as well as leaks, such as the information released by Edward Snowden, have sharply increased fears of government misconduct and privacy concerns.[82] Bulk data collection, including the collection of phone records, has drawn both strong support and fierce criticism. Supporters see technological developments as valuable means of increasing the protection of U.S. citizens and see no reason not to make use of all available advances to ensure that the United States maintains a security advantage. Critics, on the other hand, fear an irreparable trend towards minimizing privacy protections for all citizens in exchange for marginal gains in security. While these concerns are accurate and valid, so far there has been no record of abuse for personal or political gain.[83] Conversely, there has also been

[82] "Edward Snowden: Leaks that exposed U.S. spy programme" *The British Broadcasting Company* (January 17, 2014) http://www.bbc.com

[83] Jennifer Steinhauer and Jonathan Weisman, "U.S. Surveillance in Place Since 9/11 Is Sharply Limited" *The New York Times* (June 2, 2015) https://www.nytimes.com

no evidence that bulk data gathering has directly led to the thwarting of any terrorist activities.[84]

After the September 11th terrorist attacks on the World Trade Center, the United States government quickly passed legislation called the "Uniting and Strengthening America by Providing Adequate Tools Required to Intercept and Obstruct Terrorism Act of 2001," more commonly known by its acronym, the USA Patriot Act. This act of Congress, signed into law by President Bush in October 2001, greatly increased the surveillance power of the government in a frantic attempt to improve state security and combat terrorism. It allows the government to use surveillance tactics that include electronic monitoring and roving wiretaps, delaying notification of served search warrants, obtaining business records, and eliminating barriers that inhibited the sharing of information between the law enforcement, intelligence, and national defense communities. Many of these tactics were already used by law enforcement but on a much more restricted scale. The Patriot Act greatly increased the scope of government surveillance and removed restrictions that limited the use of such tactics.

These increasingly aggressive methods of information gathering eventually gave birth to the Total Information Awareness program, which was, in the words of U.S. Senator and avid privacy advocate Ron Wyden, "the biggest surveillance program in the history of the United States."[85] Later known as the 'Terror Information Awareness program' the goal of this data mining program was to gather information about people

[84] Jennifer Steinhauer and Jonathan Weisman, "U.S. Surveillance in Place Since 9/11 Is Sharply Limited" *The New York Times* (June 2, 2015) https://www.nytimes.com
[85] "Pentagon's 'Terror Information Awareness Program' will end" *USA Today* (September 25, 2003) http://usatoday30.usatoday.com

outside the United States as well as citizens on U.S. soil. The program sought out information on travel histories, credit card records, and medical records in search of patterns and signs that might indicate terrorist activity.[86] A program such as Total Information Awareness was made possible by the significant leaps in surveillance technology and the lack of regulation or transparency between the government agencies involved and the general public. When the public discovered news of the Terrorist Information Awareness program, it was publicly shut down by the government in 2004. However, in reality it was secretly continued under different codenames and eventually re-emerged as an NSA program called Planning Tool for Resource Integration, Synchronization, and Management or PRISM. The problem with a program such as this is two-fold: one, it invades the privacy of American citizens by indiscriminately collecting their information without a warrant, and two, the secrecy of it violates the trust between the government and the people it is governing because the government is spending massive amounts of money on programs the citizens neither voted on nor knew about.[87] Programs such as this are particularly damaging because they violate both the tangible and the psychological elements of privacy.

A current and poignant example of the clash between security interests and digital privacy was the recent battle between the FBI and Apple over access to data stored on Apple's iPhone during the course of an investigation into terrorist activities.[88]

---

[86] "Pentagon's 'Terror Information Awareness Program' will end" *USA Today* (September 25, 2003) http://usatoday30.usatoday.com

[87] Chris Hayes, "Before PRISM there was Total Information Awareness *MSNBC* (July 2, 2013) " http://www.msnbc.com

[88] Alina Selyukh, Camila Domonoske, "Apple, The FBI, And iPhone Encryption: A Look At What's At Stake" *National Public Radio* (February 27, 2016) http://www.npr.org/

The issue of whether or not it is a violation of the Constitution for the FBI, a federal investigatory agency, to compel Apple, a private company, to provide the government with a "back door" that bypassed the encryption security measures of the iPhone, was seemingly headed towards a monumental court battle in 2016 before being quietly dropped when the FBI found another way to access the information they sought.[89] The news of the FBI's request and the brewing court battle thrust the security vs privacy debate into the national spotlight, highlighting the role of private actors, security tools such as encryption, and the role that cell phones have played in altering our sense of privacy. Apple launched a very public campaign in favor of consumer privacy and against the development of a tool that would theoretically allow the government to access the information on any iPhone.[90] Apple recognized the importance of the FBI's security interests but expressed grave concerns about the risks of setting a dangerous precedent as well as removing the security features of a device that is used by tens of millions of people and are at the heart of protecting the vast amounts of personal information contained within the memory of the devices.[91] Our cell phones and computers are often the single biggest repositories of our personal information and granting access to that essentially eliminates any level of privacy we seek to maintain.

Finding a balance between national security and individual privacy rights is becoming progressively more complex, and the issues raised are leaving the existing

---

[89] Shara Tibken, "Apple vs FBI one year later: Still stuck in limbo" *CNET* (February 17, 2016) https://www.cnet.com

[90] See: Tim Cook "A Message to Our Customers" *Apple* (February 16, 2016) https://www.apple.com (Apple CEO's message to the public announcing Apple's commitment to its customer's privacy)

[91] "Answers to your questions about Apple and security" *Apple* (February 16, 2016) https://www.apple.com

jurisprudence and legal regulations far behind. Many of the previously developed legal doctrines and constitutional interpretations are difficult to apply to the current environment. These challenges arise from the fact that technological advancements have changed fundamental aspects of our daily lives, including the ways we interact with others and the ways in which we share information. The existing legal doctrines establish guidelines and protections based on norms and practices that simply do not exist anymore. Current concerns must address issues that are significantly different than those that existed a decade ago, let alone over a century ago.

In evaluations of the development of individuals' right to privacy, the factor consistently balancing the other side of the equation is security. The courts must find a way to assess the equally legitimate needs of both the government and the individual. The government, after all, is tasked with protecting the security of the public, which is made up of individuals. Privacy must not be eliminated or irreparably crippled by the expansion of government surveillance. Conversely, effective means of protection that assist in the protection and safety of the nation cannot be ignored in favor of privacy concerns. A compromise must be made between the two fundamental needs in order to maintain the function and integrity of our democracy. The courts must determine the reasonable and necessary extent of government surveillance as well as establish firm guidelines that outline the protection of privacy that citizens may reasonably expect to rely on. Firm regulations and guarantees for transparency are essential factors for attaining a balance that does not infringe unnecessarily on the rights of the people.

Challenges of Keeping Legal Doctrine Up to Date with Developing Technology and Society: Why the Third-Party Doctrine Fails in Today's Environment

Changes in modern society demand that the courts either develop new privacy doctrines or evolve the interpretations of the existing doctrines in such a way that they accurately reflect the modern environment they are governing. Technology and society have undergone significant changes in the time since the development of the third-party doctrine and the reasonable expectation test. As a result, the existing jurisprudence developed by the Supreme Court does not accurately reflect the issues of privacy that are relevant today. The current law leaves citizens exposed to a variety of intrusions and in the words of Senator Wyden, "Outdated laws shouldn't be an excuse for open season on tracking Americans, and owning a smartphone or fitness tracker shouldn't give the government a blank check to track your movements… Law-enforcement should be able to use GPS data, but they need to get a warrant."[92] While Senator Wyden is speaking specifically about legislation, his message holds true for the Judicial branch as well and the Supreme Court must recognize perils of this situation in their decisions. Just as the Court altered its position in 1967 through the *Katz* decision, the Court must again recognize the significance of modern developments and actively evolve its jurisprudence accordingly.

The advancements in technology during the last several decades have presented challenging scenarios for those seeking to support privacy law. The Supreme Court, a naturally slow institution that favors incremental progression rather than immediate and

[92] See: Senator Ron Wyden's speech introducing the Geolocation Privacy and Surveillance Act (GPS Act) co-sponsored by Representative Chaffetz and Representative Conyers. (February 15, 2017) Portions of the speech were found on his website www.wyden.senate.gov

broad responses to new issues, has been slow to demonstrate recognition of the shortcomings of the existing doctrines. Particular justices such as Justices Stevens, Douglas, Marshall, and Sotomayor, who have demonstrated a special attention to the threats technology poses for fundamental privacy rights, have expressed their concerns. However, despite the seriousness of their concerns, these scattered instances of prudent foresight have nearly always lacked the support of the majority of the Court. In those instances when the Court does deliver an opinion that supports privacy rights and protects personal information from intrusion, it is almost always narrow in scope and relies heavily on the Court's incremental nature, following the given circumstances of the situation rather than the notion that a foundational shift in jurisprudence is needed.

This is clearly seen in the narrow focus of some of the Court's most recent decisions regarding privacy rights such as *United States v. Jones*[93] and *Riley v. California*.[94] In each of these particular decisions, the Court articulated bright line boundaries determining that particular actions such as placing a GPS device on a car and recording the locations it travels over a long period of time and the searching of the digital content of an arrestee's cell phone during the arrest constitute a violation of the Fourth Amendment. Although these decisions demonstrated support for preserving individuals' right to privacy as intended by the original purpose of the Fourth Amendment, they failed to address the larger extent of the issue that expands beyond the narrow framework of the particular facts of the cases. And most importantly, the

[93] See: *U.S. v. Jones,* 565 U.S. (2012) (An overall evaluation of the Court's opinion suggests a narrow focus that is limited by the facts of the case)
[94] See: *Riley v. California,* 573 U.S. (2014) (An overall evaluation of the Court's opinion suggests a narrow focus that is limited by the facts of the case)

Court continued to neglect the ultimate need for the introduction of a refreshed interpretation of the Fourth Amendment. Just as the Court adopted the reasonable expectation test in the 1960's as a way to recognize changing norms of communication and the integration of the telephone into daily use, the Court is again faced with a pressing need for a comprehensive change or addition to its methods of interpretation or application of privacy doctrine.

The current jurisprudence focusses heavily on the situational facts of an incident rather than the particular information in question. For the most part, the Court has treated all types of information the same. Based on a rigid interpretation of the third-party doctrine, the Supreme Court has held that information of varying levels of importance ranging from incriminating documents given to an attorney by a defendant (*Fisher v United States*[95]), to telephone numbers transmitted to a telephone company (*Smith v. Maryland*[96]), to personal financial information recorded by a bank (*California Bankers Association v. Shultz*[97]) all possess zero protection under the Fourth Amendment simply because of the common factor that in these situations the information is not in the hands of the individual who holds the privacy interest. This is deeply problematic because most individuals would almost certainly prioritize the protection of incriminating papers or even financial records over the numbers he or she dials into a telephone. It is both reasonable and entirely logical to prioritize the

[95] See: *Fisher v. United States* 425 U.S. 391 (1976) (This decision addresses the confidentiality of documents shared between a lawyer and their client)
[96] See: *Smith v. Maryland,* 442 U.S. 735 (1975) (This decision addresses the confidentiality of information, such as telephone numbers, that is voluntarily transmitted to a telephone company)
[97] See: *California Bankers Association v. Shultz* 416 U.S. 21 (1974) (This decision addresses the confidentiality of information, such as bank records, that are recorded and held by banks)

protection of one's personal information based on its value to the individual and the potential for harm should it be discovered and used for malicious purposes; however, this is not the current position of the Supreme Court.

In theory, this doctrine has been a relatively good benchmark for establishing a person's expectation of privacy because, logically, if a person is willing to share information, then they must not be interested in keeping it a secret. However, in the modern world, it is inadequate because it ignores of the basic level of information sharing that takes place through normal day-to-day activities such as online searching and shopping or communicating through text, call, or email. These are simple activities that most of us would consider essential in order to be a contributing member of modern society. The third-party doctrine's assumption of a relinquished privacy interest by any individual who engages in these types of transactions ignores the modern developments that have connected the world in such a way that sharing basic personal information in this manner is a necessary, frequent, and unavoidable reality.

Private Access vs. Government Access: Who Gets Access to Information and in What Situations

In *Kyllo v. United States*, Justice Scalia engaged the increasingly important issue of the government's ability to access information vs the general public's or private entity's ability to access information. In the *Kyllo* decision, the Court determined that the government should not be able to use technology that was not yet in use by the general public to learn previously unknowable information about a home — at least without a warrant. This is an important position to understand. Justice Scalia was intent

on ensuring that the government and its agents were not able to use new technologies to erode the protections of the Fourth Amendment.

In the years since the *Kyllo* case, technologies used by private individuals or by particularly cutting-edge companies, have largely become more advanced than the resources of most police forces. Private individuals who follow our social media profiles are privy to our habits, interests, daily activities, and even our location. Companies such as Google know and record our online search histories, which can reveal any number of details or insights into who we are as a person. Cellular providers such as Verizon, AT&T, and Sprint have access to our calls, text messages, and location data. Online retailers such as Amazon have records of our shopping history and lifestyle preferences. These privately-owned companies record and store massive amounts of this data. Usually this data is used internally by the companies to improve the quality of their services and even tailor their service to the individual needs of each user.[98] Companies also sell this coveted data to advertisers who seek to increase the efficiency of their advertising and marketing strategies by targeting specific audiences based on indicators located in their browsing histories. As consumers, we have come to appreciate these improved and personalized services, but we often ignore the cost at which these improvements come.

Even if companies are not tracking sensitive personal information such as medical records, religious preferences, or sexual tendencies, there are still unexpected and objectionable ways in which they can use your Internet history. Using a practice

[98] Nathan Wessler, "How Private is Your Online Search History?" *American Civil Liberties Union* (November 12, 2013) https://www.aclu.org

known as "dynamic pricing" companies adjust their prices on the fly using software algorithms that take into account factors such as time, location, and competitors prices.[99] Usually these factors are relatively benign and allow the companies to market their goods more competitive to consumers. Dynamic pricing is legal; however, it can quickly become problematic when there are also other lesser known factors that companies can track and use to target unsuspecting consumers. These often include browsing histories and even which browser an individual is using. The online travel agency, Orbitz, was recently caught up-selling their travel packages based on the browser the customer was using. It was discovered that Orbitz was displaying pricier hotel options to users operating Safari (Mac) over their Internet Explorer (PC) counterparts.[100] [101] Orbitz was doing this based on the notion that Mac users are more affluent than PC users and will therefore pay more for a hotel or travel package. While this is not entirely surprising, and not an invasion of intimate information, it highlights the ways in which private companies are tracking users' online information and activity for profiling purposes that eventually lead to problematic practices.

Increased private access to personal information becomes even more precarious when it expands beyond simply advertising and marketing purposes and beings to include information that has potential criminal, political, religious, or sexual implications. As part of an NPR series focusing on individuals' digital trails and who can access them, a digital privacy specialist named Ashkan Soltani demonstrated how

---

[99] Margaret Rouse, "Dynamic Pricing" *WhatIs.com* (December 2015) http://whatis.techtarget.com
[100] Elinor Mills, "How to outfox Web sites trying to get you to pay top dollar" *CNET* (June 26, 2012) http://news.cnet.com
[101] Ashkan Soltani, "Protecting Your Privacy Could Make You The Bad Guy" *Wired* (July 23, 2013) https://www.wired.com

changing social norms have encouraged information sharing and how private companies track this information.[102] He created a fake account on OKCupid.com (an online dating and relationship website). He filled out their questionnaire, voluntarily offering information such as: gender, age, income, religion, ethnicity, political leanings, and even his alcohol and drug use habits. He then used two software programs (Collusion and MITM Proxy) which reveal that nearly 50 companies are monitoring his computer's activity on the OKCupid website. According to Soltani's software, not all of the companies were receiving all of the data, some were only tracking his age and gender information while others were recording all of his activity, including the information about his drug and alcohol use.[103] Research says it is common for third-party companies to monitor a user's activity across websites, effectively creating a visual thumbprint of a user's online activity.[104] [105] While much of this information is used for marketing and advertising purposes and not for malicious purposes, it is fundamentally changing the notion of privacy because, regardless of the purpose, the information is held by someone other than the individual to whom it pertains.

The problem is further compounded by the rift between private entities and the government, because security agencies in the government would like to have access to the same information that the private companies have access to but are limited by the

[102] Daniel Zwerdling, "Your Digital Trail: Private Company Access" *National Public Radio* (October 1, 2013) http://www.npr.org
[103] Daniel Zwerdling, "Your Digital Trail: Private Company Access" *National Public Radio* (October 1, 2013) http://www.npr.org
[104] Daniel Zwerdling, "Your Digital Trail: Private Company Access" *National Public Radio* (October 1, 2013) http://www.npr.org
[105] "The Murky World of Third Party Web Tracking" *MIT Technology Review* (September 12, 2014) https://www.technologyreview.com

Constitution whereas the private companies are not. The question becomes, with regard to privacy rights, should the government be limited to the tools and resources that are considered within the general public use? The discussion is incredibly complicated, largely because the technological environment we are faced with today is very different than the one that existed less than two decades ago when *Kyllo* was decided and it was determined that the government should not be able to use technology or devices for the purpose of investigation or discovery that were not commonly used by the general public. Individuals in the general public and publicly owned companies now have increasingly high levels of access to the intimate details of our lives, levels of access that become troubling if the legal standard is to expect the government to have the same levels of access that are available to our peers or to companies.

Since the 2001 *Kyllo* decision, technology has continued to develop at an even greater pace; companies have continued to integrate themselves into our daily lives and connect the global community in new ways; and finally, the security threats facing us have become more dangerous and more difficult to detect. In an effort to stay ahead of increasingly complex threats such as terrorism and cyber-attacks, government agencies such as the NSA and the FBI have developed massive surveillance programs, some of which operate in conjunction with private companies such as Google, Facebook, Microsoft, and Apple. The government uses information compiled by these companies to monitor the general public.[106] The cooperation between investigative government agencies and companies with which we voluntarily share private information in the

[106] Kaveh Waddell, "The NSA's Bulk Collection Is Over, but Google and Facebook Are Still In The Data Business" *The Atlantic* (June 3, 2015) https://www.theatlantic.com

context of daily activities and narrowly defined business purposes is inherently troubling. It is troubling because the information we provide these companies is being used by both the companies and government for purposes that were not originally intended and in ways that circumvent our fundamental protections against unwanted government invasion.

Distinguishing between government access and private access is an important step in curbing government access to personal information held by private sector entities. It is clear that private corporations have reached a level of integration into our lives that is well beyond the reasonable scope of government intrusion. Therefore, it is unreasonable and unconstitutional for government agencies to continue to have the same relatively easy access to the information compiled by these private actors that they have previously enjoyed. This is not to ignore the value of such information to the government agencies seeking to provide security for our nation, but it is to implement a necessary protection against the indiscriminate vacuuming of the information of all citizens indifferent of specified suspicion of criminal wrongdoing. The standard must be raised to that of "probable cause" and require the granting of a warrant before the government may request information held by private companies. This way government agencies may still conduct surveillance and access the necessary information, but on a much more defined and targeted basis.

Psychological Dimensions of Privacy

Privacy is primarily thought of in terms of as a tangible protection against the prying eyes and ears of those who seek to uncover information that some individual

desires to keep private; however, that is only part of what privacy entails. Privacy also includes valuable psychological aspects that are essential to the well-being of the individual, as well as fundamental in the bond of trust between a democratic government and its citizenry. The intrinsic desire for personal space and the peace of mind that accompanies the assurance that there are places and situations in which we are free from unwanted intrusion is important on both an individual level and on a political level. At the personal level, the ability of the individual to maintain the privacy of his personal affairs is central to the American ideals of individualism an autonomy. While at the governmental level, the bond between the government and the citizenry dictates that a reciprocal trust must exist so that each may fulfill its prescribed duties: the government's duty to represent the interests and protect the rights of the citizens, and the electorate's responsibility to legitimize government authority through free and informed decisions. The government must trust the citizens to exercise their liberties responsibly and respect their right to maintain privacy within their lives, or risk disintegrating the bond of trust and slipping towards a totalitarian regime based on power and fear. "It is the second area of trust—trust that the citizenry will exercise its liberties responsibly— that implicates the Fourth Amendment and is jeopardized when the government is allowed to intrude into the citizenry's lives without finding that the citizenry has forfeited society's trust to exercise its freedoms responsibly."[107]

Privacy centers around one's expectation of having it, meaning that the psychological value of privacy relies on what most people can reasonably expect to be

[107] Scott E. Sundby, "'Everyman's' Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?" *Columbia Law Review,* 1751 Vol. 94 no. 6 (October, 1994) : 1777

private, or conversely, what most people expect to be public. This psychological expectation of privacy is exceptionally difficult to establish in an increasingly non-private world. Simply put, "a Fourth Amendment based on expectations of privacy must contend with the changing nature of modern society. The very notion of the right to be left alone seems a bit tattered once placed next to the context of contemporary life… we may want to be left alone, but we realistically do not expect it to happen in any complete sense."[108] As news of government surveillance becomes increasingly prevalent, particularly after the leaks by Edward Snowden, American citizens have a growing expectation that the government is constantly watching their every move.[109] There is a recognizable shift in the psychology of Americans as a general acceptance of a widespread loss of privacy begins to take hold as the norm. This is extremely problematic in terms of privacy because a deteriorating expectation of privacy significantly damages its overall purpose.

The implications of a change in privacy, particularly the psychological aspects, are harmful both to individuals and to government as a whole. A fundamental deterioration in people's expectation of privacy creates a "chilling effect" on their freedom of association and intimate relations as well as their freedom of expression and action in both personal and political contextes. This effect was exemplified in a study examining the internet traffic patterns of privacy sensitive webpages before and after the Snowden leaks revealing the extent of surveillance programs such as PRISM. The

[108] Scott E. Sundby, "'Everyman's' Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?" *Columbia Law Review,* 1751 Vol. 94 no. 6 (October, 1994) : 1758-1759
[109] "Edward Snowden: Leaks that exposed U.S. spy programme" *The British Broadcasting Company* (January 17, 2014) http://www.bbc.com

study concluded that there was a 30 percent drop in traffic for these sites after the disclosure of the government programs, thus empirically confirming the existence of a chilling effect.[110] While this specific instance may not seem to have much importance, the larger implications are gravely serious. It confirms that knowledge of the government surveillance programs is directly related to a diminishing expectation of privacy and has a direct impact on the actions of the citizenry. This threatens to disrupt the bond of trust between government and constituency, resulting in significant political and societal implications.

[110] Andrew Blake, "NSA surveillance had chilling effect on Internet browsing: report" *The Washington Times* (April 27, 2016) http://www.washingtontimes.com

Conclusion

Adapting privacy law to the needs of the digital age is not simple or straightforward by any stretch of the imagination. It is clear that privacy is a complex concept that has evolved in response to societal changes and expectations. It has been influenced by legal interpretation, technological development, social integration, and psychological shifts in society. In recent years, pressures such as increasingly complex security risks and technological advancements that outpace legal doctrines have created an environment in which privacy is an ambiguous and precarious right. There may be no singular solution to the various faults in privacy law, but there are several specific steps that can help initiate movement in a direction that stabilizes the foundation of the right to privacy and establishes an adequate platform from which clear protections can be extended. A firm foundation and clear protections are necessary to ensure the privacy of individuals' personal information, in an environment that increasingly encourages access to private information and personal details of one's life.

The Court must address the outdated doctrines and jurisprudence used to guide its decision making on privacy issues. Justice Sotomayor has already hinted in her *Jones* concurrence that she is ready to encourage the Court to revisit the third-party doctrine and refresh its view of that standard. In order to make the third-party doctrine effective in the digital age where personal information is frequently shared during everyday transactions and interactions, the Court must address the different types of information shared and in what context they are shared. The simple fact that an individual passes previously confidential information to a third-party should no longer mean that

confidentiality is immediately lost. This purely situational approach that relies on a bright line test is outdated and is ineffective in protecting the privacy of information.

The Court must recognize in its future decisions that we as individuals are interconnected like never before, and therefore there must be elements of shared privacy between certain individuals or entities regarding particular types of information that are taken into account by the law.[111] The law should be advanced to maintain the confidentiality of information shared within certain transactional contexts of limited and specifically defined business interests, such as health and financial information. Another approach might include recognizing differing levels of privacy based on the content of the information in question. For instance, the metadata collected by cellular companies such as the time and duration of phone calls, to whom the phone call was placed, and the location the calls were placed from may have a lower level of privacy than the content information, which would consist of what was said during the call or the words of text messages. However, this is a particularly challenging argument because given the quantity of metadata that can now be compiled and analyzed, it is possible for someone to develop nearly as clear of an understanding of another person's personal information through metadata as they might otherwise develop by reading the content of personal messages. Records such as search histories and purchase histories present a unique challenge in terms of distinguishing between content information and metadata. This is because a search is unique in that it is not a communication between two people, but still communicates individualized information to a third-party. Each person's

[111] Mary Coombs, "Shared Privacy and the Fourth Amendment, or the Rights of Relationships" *California Law Review* 1593 Vol. 75 no. 5 (October, 1987) : 1597

history is often extremely personal, and if collected over a long enough period of time, can reveal the most intimate details of their life such as sexual orientation, political and religious affiliations, medical concerns, and financial habits.

Based on these concerns, the third-party doctrine should no longer be used as a tool by the government to gain access to people's private records that they have no choice but to share with companies such as their cellular and internet providers, banks, or healthcare institutions. Instead, a comprehensive approach should be adopted that takes into account the realities of the integrated world we live in where confidential information is shared and should continue to maintain its confidential status. The removal of the bright line test, and the implementation of a balanced approach that recognizes varying levels of privacy based on the type of content or data as well as the context in which it was shared are necessary steps to take in order to restore protection and peace of mind to the average American. A failure to do this will continue our current trajectory down a slippery slope towards a total surveillance state in which average individuals are stripped of their privacy and autonomy and government influence reigns supreme — an environment not dissimilar to the dystopian world described in George Orwell's novel *1984*. The effects of such an environment on the psychology of individuals as well as the collective identity of the general population are ominous. That is why it is imperative that definitive steps are taken soon to reverse the trend towards increased government intrusion, and ensure clear legal protections for individuals' privacy. Changing the outdated and inadequate doctrines in favor of ones that are consistent with the technological and societal norms of the current era is of the utmost importance.

Finally, the most challenging aspect of advancing privacy rights is balancing the security needs of the government with the privacy needs of the general population. There is an overarching belief that ensuring the safety and security of the nation is one of the foremost priorities of the government, but the important question remains, what level of government surveillance and infringement of privacy is an acceptable trade-off for increased security? The threats that face the United States are becoming increasingly complex, in the forms of both foreign and domestic terrorism as well as cyber-attacks that threaten our electronic infrastructure and the databases of important government agencies. In an effort to combat these threats, the government has engaged in measures to proactively detect and prevent suspicious activity.

This includes increased surveillance and electronic monitoring of communications and information on a widespread scale. While reports claim that these monitoring efforts have been successful in deterring and thwarting numerous threats, they have also received heavy criticism for infringing upon the liberty and privacy of the people.[112]

To effectively achieve adequate security, some level of surveillance and monitoring by the government is necessary; however, it does not have to be entirely at the expense of the privacy of the people. Increased transparency as well clear explanations of the intent of the surveillance and the guidelines for conducting the surveillance need to be laid out and adhered to, in order to maintain the trust of the citizens and to ensure that privacy protections are continued. This will likely take a

[112] Jennifer Steinhauer and Jonathan Weisman, "U.S. Surveillance in Place Since 9/11 Is Sharply Limited" *The New York Times* (June 2, 2015) https://www.nytimes.com

combined effort from the courts as well as the legislature. Action may take place first in lower level courts and in the state legislatures before reaching Congress and the Supreme Court.

A potential solution is to implement varying levels of scrutiny for different types of surveillance. The government might be allowed to have relatively easy access to pure data information but demonstrate a higher level of suspicion and urgency in order to access content information. This would allow surveillance to continue, but with situational and content factors limiting what the government has access to and for what reasons. Allowing government agents to continue to monitor data and limited elements of communications by searching for suspicious keywords or communication patterns is essential to the function of agents protecting our safety, and it does not unduly infringe upon the privacy of individuals.

Further investigation into specific suspects would require the government to demonstrate a higher standard such as a compelling interest or reasonable suspicion as well as a narrowly tailored scope of investigation. The goal is not to create an environment in which the government agencies seeking to protect the country are inhibited from doing their job, but rather to create clear guidelines within which they can operate, while removing the ambiguity as to individuals' privacy and providing certain guarantees of privacy protection.

This logic also applies to the increasing government partnership with private companies to gain access to and comb through the private records compiled by the companies. Companies such as Google, Yahoo, Facebook, Verizon, and Apple have become integrated into our daily lives and have access to far more personal information

than government agencies like the FBI have access to. Therefore, the government has used the third-party doctrine to gain easier access (requiring a subpoena rather than a warrant) to the information compiled by these companies by their users. This violates the privacy of the users because they did not convey the information with the intent of it being used beyond the scope of the narrow business interaction for which they supplied it. Apple has taken steps to fight back against FBI requests for the creation of a backdoor to the encryption code of the iPhone.[113]

It is important for companies to follow Apple's example and take a firm stand against government efforts to invade the privacy of their users. Of course, assistance from these companies is an important part of the government's efforts to detect threats to national security early and prevent them, but there must be limits on the lengths that the government can go to in order to achieve its ends. Access to any information held by these companies should require that the government demonstrate at the very least reasonable suspicion, and perhaps a compelling interest in instances including content information. Investigations should also be narrowly tailored and clearly defined so that the expectations and intentions are unambiguous.

Privacy is a core aspect of our fundamental needs as individuals and as a democratic society. We are a society of laws and we must advance these laws to keep pace with the changes and demands of the world we live in. Allowing our tangible and psychological value of privacy to be diminished by our infatuation with the latest and greatest technological advancement or the newest development in personalized service

[113] Danny Yadron, Spencer Ackerman, and Sam Theielman "Inside the FBI's encryption battle with Apple" *The Guardian* (February 18, 2016) https://www.theguardian.com

or even the repeated promise of increased security is something we cannot allow. We must stand firm and defend our right to privacy because it is a fundamental legal right, an essential element of psychological wellbeing, and finally a core pillar of American ideology.

Supreme Court Cases

Boyd v. United States, 116 U.S. (1886)

California Bankers Association v. Shultz, 416 U.S. (1974)

Chimel v. California, 395 U.S. (1969)

Fisher v. United States 425 U.S. 391 (1976)

Griswold v. Connecticut, 381 U.S. (1965)

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

Kyllo v. United States, 533 U.S. (2001)

McDonald v. Chicago, 561 U.S. (2010)

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

Riley v. California, 573 U.S. (2014)

Smith v. Maryland, 442 U.S. (1979)

United States v. Jones, 565 U.S. 945 (2012)

United States v. Miller, 425 U.S. (1976)

Bibliography

Barkow, Anthony. "Symposium: A whole lot of Wurie: Information acquisition and the Fourth Amendment." SCOTUSblog. June 26, 2014. http://www.scotusblog.com/2014/06/symposium-a-whole-lot-of-wurie-information-acquisition-and-the-fourth-amendment/.

Blake, Andrew. "NSA surveillance has had chilling effect on Internet browsing: report." The Washington Times. April 27, 2016. https://www.washingtontimes.com/news/2016/apr/27/nsa-surveillance-has-had-chilling-effect-internet-/.

Cohen, Julie E. "What is privacy for." *Harvard Law Review* 126 (November 5, 2012).

Cook, Tim. "Customer Letter." Apple. February 16, 2016. https://www.apple.com/customer-letter/.

Coombs, Mary I. "Shared Privacy and the Fourth Amendment, or the Rights of Relationships." *California Law Review* 75, no. 5 (1987): 1593. doi:10.2307/3480488.

"Customer Letter - FAQ." Apple. February 16, 2016. https://www.apple.com/customer-letter/answers/.

"Edward Snowden: Leaks that exposed US spy programme." BBC News. January 17, 2014. http://www.bbc.com/news/world-us-canada-23123964.

Friedman, Barry, and Orin Kerr. "The 4th Amendment of the U.S. Constitution." National Constitution Center – The 4th Amendment of the U.S. Constitution. Accessed December 06, 2017. https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv.

Hartzog, Woodrow, and Evan Selinger. "Obscurity: A better way to think about your data than 'privacy.'" *The Atlantic*, January 17, 2013. https://www.theatlantic.com/technology/archive/2013/01/obscurity-a-better-way-to-think-about-your-data-than-privacy/267283/.

Hayes, Chris. "Before PRISM there was Total Information Awareness." MSNBC. September 12, 2013. http://www.msnbc.com/all-in/prism-there-was-total-information-awar.

"History." Justia Law. Accessed December 06, 2017. https://law.justia.com/constitution/us/amendment-04/01-search-and-seizure.html.

"Katz v. United States: The Fourth Amendment adapts to new technology." National Constitution Center – constitutioncenter.org. https://constitutioncenter.org/blog/katz-v-united-states-the-fourth-amendment-adapts-to-new-technology/.

Kerr, Orin. "Opinion | Supreme Court agrees to hear 'Carpenter v. United States,' the Fourth Amendment historical cell-site case." The Washington Post. June 05, 2017. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/05/supreme-court-agrees-to-hear-carpenter-v-united-states-the-fourth-amendment-historical-cell-site-case/.

Kiralfy, Albert Roland, Andrew D.E. Lewis, and Mary Ann Glendon. "Common law." Encyclopedia Britannica. October 26, 2017. Accessed December 06, 2017. https://www.britannica.com/topic/common-law.

Lee, Timothy B. "Here's everything we know about PRISM to date." The Washington Post. June 12, 2013. https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

Markowsky, George. "Misconceptions about the Golden Ratio." *The College Mathematics Journal* 23, no. 1 (1992): 2-19. doi:10.2307/2686193.

Mills, Elinor. "How to outfox Web sites trying to get you to pay top dollar." CNET. June 26, 2012. https://www.cnet.com/how-to/how-to-outfox-web-sites-trying-to-get-you-to-pay-top-dollar/.

"Negligence." The Free Dictionary. https://legal-dictionary.thefreedictionary.com/negligence.

"Oyez." Oyez. Accessed December 06, 2017. https://www.oyez.org/.

"Pentagon's 'Terror Information Awareness' program will end." USATODAY.com. September 25, 2003. http://infolab.stanford.edu/~ullman/fcdb/aut07/2006/ethics_readings/USA-Today-TIA-cancelled.htm.

"Reasonable Person." The Free Dictionary. Accessed December 06, 2017. https://legal-dictionary.thefreedictionary.com/reasonable person.

Rouse, Margaret. "What is dynamic pricing? - Definition from WhatIs.com." WhatIs.com. December 2015. http://whatis.techtarget.com/definition/dynamic-pricing.

"Search and Seizure." Search and Seizure. Accessed December 06, 2017. http://www.searchandseizure.org/.

"Search Warrants: What They Are and When They're Necessary." Www.nolo.com. Accessed December 06, 2017. https://www.nolo.com/legal-encyclopedia/search-warrant-basics-29742.html.

Selyukh, Alina, and Camila Domonoske. "Apple, The FBI And iPhone Encryption: A Look At What's At Stake." NPR. February 17, 2016. https://www.npr.org/sections/thetwo-way/2016/02/17/467096705/apple-the-fbi-and-iphone-encryption-a-look-at-whats-at-stake.

Solon, Olivia. "Your browsing history may be up for sale soon. Here's what you need to know." *The Guardian*, March 28, 2017. https://www.theguardian.com/technology/2017/mar/28/internet-service-providers-sell-browsing-history-house-vote.

Soltani, Ashkan. "Protecting Your Privacy Could Make You the Bad Guy." Wired. June 03, 2017. https://www.wired.com/2013/07/the-catch-22-of-internet-commerce-and-privacy-could-mean-youre-the-bad-guy/.

Staff, LII. "Fourth Amendment: Warrantless Searches Incident to Arrest." LII / Legal Information Institute. July 17, 2014. https://www.law.cornell.edu/supct/cert/supreme_court_2013-2014_term_highlights/fourth_amendment_warrantless_searches_incident_to_arrest.

Steinhauer, Jennifer, and Jonathan Weisman. "U.S. Surveillance in Place Since 9/11 Is Sharply Limited." The New York Times. June 02, 2015. https://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html.

Sundby, Scott E. "Everyman's Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?" *Columbia Law Review* 94, no. 6 (October 1994): 1751. doi:10.2307/1123178.

"The 4th Amendment of the U.S. Constitution." National Constitution Center – The 4th Amendment of the U.S. Constitution. Accessed December 06, 2017. https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv.

"The Murky World of Third Party Web Tracking." MIT Technology Review. September 19, 2014. https://www.technologyreview.com/s/530741/the-murky-world-of-third-party-web-tracking/.

Tibken, Shara. “Apple's battle with the FBI leaves lingering questions.” CNET. February 15, 2017. https://www.cnet.com/news/apple-vs-fbi-one-year-later-still-stuck-in-limbo/.

Waddell, Kaveh. “The NSA's Bulk Collection Is Over, but Google and Facebook Are Still in the Data Business.” The Atlantic. June 03, 2015. https://www.theatlantic.com/politics/archive/2015/06/the-nsas-bulk-collection-is-over-but-google-and-facebook-are-still-in-the-data-business/458496/.

Warren, Samuel D., and Louis D. Brandeis. “The Right to Privacy.” *Harvard Law Review* 4, no. 5 (1890): 193. doi:10.2307/1321160.

Wessler, Nathan Freed. “How Private is Your Online Search History?” American Civil Liberties Union. April 26, 2015. https://www.aclu.org/blog/national-security/how-private-your-online-search-history.

Wyden, Ron. “In Speech to Cato, Wyden Calls for Modernizing Law, Providing Clarity on Geolocation | Senator Ron Wyden.” Senator Wyden. January 26, 2011. https://www.wyden.senate.gov/news/press-releases/in-speech-to-cato-wyden-calls-for-modernizing-law-providing-clarity-on-geolocation.

Yadron, Danny, Spencer Ackerman, and Sam Thielman. “Inside the FBI's encryption battle with Apple.” The Guardian. February 18, 2016. https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple.

Zwerdling, Daniel. “Your Digital Trail: Private Company Access.” NPR. October 01, 2013. https://www.npr.org/sections/alltechconsidered/2013/10/01/227776072/your-digital-trail-private-company-access.

“Fourth Amendment: Search and Seizure – History and Scope of the Amendment.” Justia Law. Accessed December 06, 2017. https://law.justia.com/constitution/us/amendment-04/01-search-and-seizure.html.