AN ANALYSIS OF THE EXPECTATION OF PRIVACY IN THE UNITED STATES:

EMPHASIS IN MODERN LEGAL RULES

By

ZOE R. MESSER

A Thesis Submitted to the Honors College

In Partial Fulfillment of the Bachelors degree

With Honors in

Law

THE UNIVERSITY OF ARIZONA

MAY 2017

Approved by:

____________________________

Robert A. Williams, Jr.
E. Thomas Sullivan Professor of Law
Abstract

The Age of Data has quickly constructed a world where secrecy is a myth and privacy is an idea clouded in insecurity and dishonesty. In this Thesis, I explore the realm of “privacy” and its different contextual meanings. Relying on various sources to expand on privacy, I will view the issue of privacy in American social, historical, governmental, and most importantly, legal contexts. I will be using modern terms such as Big Data, metadata, and “The Surveillance State” to narrow down our understanding of why privacy is important and how these terms have created an entirely different way of thinking about the world. Can our everyday data use (i.e. text messages, phone calls, internet search history) be infringed upon? If so, on what legal grounds? Traditional and modern privacy concerns are important to acknowledge here as well. Further research, backed by history, relevant literature, and modern legal rules, is especially vital to our understanding of data as a private “thing,” how privacy is protected, and whether we are willing to give our privacy away. Is there an expectation of privacy in America today that embraces everything we want kept private?
Statement of Purpose

The purpose of this Thesis is to examine the definitions, practices, and potential problems with our claim to privacy in America. Much of our population is completely unaware that no citizen has the expressed “right” to privacy laid out in our Constitution. Our implied rights are interpreted differently based on the audience. The topic of this Thesis is very relevant to the current political and social climate. I would like to use this essay as a resource for those seeking an understanding of one of the most broad—and complex—topics of our time.

Objective

My objective is to section this Thesis into three broad topics: privacy, property as data and its collection, and surveillance in America. Within each section I will explain what the three topics are, how the topics may be applied to the world today, and identify any potential problems that may arise in the application of each one.
“Privacy is the right to enjoy the product of our own intellect. Privacy is the fountainhead of all other rights. Privacy is the right to the self. Privacy is the right to a free mind.”

—Edward Snowden

**Privacy: One Word, Endless Meanings**

Privacy cannot have one single definition—it was never meant to. Privacy is viewed through various lenses every day and may look radically different through each one. The original context for the “right to privacy” in America comes from the United States Constitution and over 200 years of federal litigation broadening the scope of the law to what we follow today. In my research, I have set out to find the various definitions of privacy which may aid in the understanding of how privacy has affected our lives.

In a survey, I administered in the Fall of 2016, I asked participants to describe what privacy means to them. The responses consisted of relatively similar prose, such as “Privacy is the absence of uninvited eyes and ears in my personal business,” “No one knows unless I tell them,” and “Having the right to withhold personal information and interactions.” These personal definitions give a sense of how the idea of privacy has been internalized throughout our lives. After reading close to 60 responses from a wide variety of age groups and levels of education, I gathered a strong sense of entitlement from each person. What I mean by “entitlement” is that the vast majority of responses to this specific question weren’t done with much reflection. The responses were written as if this question was something they had already made up their mind about in one way or another. Whatever the case, the universal interpretation of privacy is that we

---


somehow deserve it… and that may not necessarily be true. The question remains, are these definitions accurate? Are they enough to prove that privacy is a fundamental right? To answer these, I have looked to more reliable sources in both professional and legal contexts.

Beginning in one of the most appropriate places to find a definition, I searched for “privacy” in Black’s Law Dictionary which lays out the definitions of privacy in four categories:

(1) Physical: An imposition whereby another individual is restricted from experiencing an individual or a situation. (2) Decisional: The imposition of a restriction that is exclusive to an entity. (3) Informational: The prevention of searching for unknown information and (4) Dispositional: The prevention of attempts made to get to know the state of mind of an individual.

An extended definition such as this one makes it abundantly clear that privacy and its practices come with a wide range of interpretations. Of course, these interpretations make perfect sense as there are numerous ways to handle the concept of privacy or lack thereof. As shown above, someone may have physical privacy in the clothes they wear and the parts of their body they chose to remain hidden or covered. Someone may have decisional privacy, which protects them from interferences of outside influence on their own rationale. Someone may also have dispositional privacy, which is essentially privacy of thought. Perhaps the most relevant distinction of privacy to our time is privacy of information.

A passage excerpted from a Duke Law review says, “Privacy is a concept in disarray. Nobody can articulate what it means. As one commentator has observed, privacy suffers from ‘an embarrassment of meanings.’ Privacy is far too vague a concept to guide adjudication and law-making…”

---


the outcome of cases that provide an overextended definition of what privacy should be, rather than what privacy actually is.

**Constitutional Implications of Privacy**

There are roughly 7,500 words on the 4 sheets of the Constitution including the 27 Amendments. Compare this to the average 36,000 worded State Constitutions in America. In the past 200 years, there has been a lot of diverse interpretations of the U.S. Constitution, most of which take a certain phrase or wording and assume it means something by extension. This is called implied powers, or implied rights. Implied rights are rights or powers that are not expressly granted in writing, but can be assumed from the text that a certain right exists.

The right to privacy is exactly one of those rights, and conceivably the most famous and hotly debated of them all. Consider the Fourth Amendment, which has been used to explain Constitutional privacy rights. The Fourth Amendment says that “each person has a protection from unreasonable search and seizure…which includes arbitrary arrests, and is the basis of law that justifies search warrants…wiretaps, and other forms of surveillance… and is central to privacy law.”

The Fourth Amendment’s reach is far and extensive. The Amendment says, “The right of the people to be secure in their persons, houses, papers, and effects…shall not be violated” This sentence is vital to understand what is exactly protected under the Fourth Amendment. According to the wording of the Fourth Amendment, there are only four things that are protected. Over the last 200 years, American Law has been able to place certain things under

---

5 LII/ Legal Information Institute. n.d. *Fourth Amendment.*
6 Ibid.
each of those categories. For example, the right to be “secure in their houses” means more than only the protection of the house’s foundation, walls, and roof. By extension, this means that the items inside the house are also protected. The phrase “a man’s home is his castle” has been continuously applied to the protection of houses because a home is essentially an extension of oneself, holding valuable and personal property. Therefore, to arbitrarily and unreasonably search a home is a direct violation of the Fourth Amendment.

The dilemma that Constitutional Law faces today is how far the Fourth Amendment will go in protecting “persons, houses, papers, and effects.” We know today that our personal property is more valuable than ever, and what we consider property, another person may not. Consider the Olmstead v. United States case from 1928, where the Supreme Court was presented with an issue of the use of police wiretapping without judicial consent and used as evidence against the plaintiffs, Roy Olmstead, amongst others. The plaintiff believed that his Fourth and Fifth Amendments were violated, however law enforcement never gained physical entry into the plaintiff’s home.

Justice Howard Taft delivered the majority decision, which said that “wiretapping was not protected by the Fourth Amendment. There was no search, there was no seizure, only the use of the sense of hearing. There was no entry of the houses or offices of the defendants.” Justice Louis Brandeis delivered the controversial dissent to this case, which said that the “Fourth and Fifth amendments must be capable of wider application then the mischief which gave it birth.” Justice Brandeis understood that this type of right must move with the times, or else the government will not be limited as to what they can do. The creation, access, and use of new

___ LII/ Legal Information Institute. n.d. Fourth Amendment.
8 Olmstead v. United States, 277 U.S. 438 (1928)
9 Ibid.
technologies were becoming more relevant and Brandeis believed that it would be ridiculous for the courts not to acknowledge that fact.

Moving back in time a few decades, Justice Brandeis and his close friend and colleague Justice Samuel Warren had a firm grasp, even in 1890, on the issue of property and affirmed that the right to “life, liberty, and property” granted in the Fourteenth Amendment could evolve to mean almost anything. Justices Brandeis and Warren, two of the most forward-thinking justices ever to sit on the court said,

…in very early times, the law gave a remedy only for physical interference with life and property…Later, there came a recognition of man’s spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life, the right to be let alone, the right to liberty through civil privileges; and the term ‘property’ has grown to comprise every form of possession—intangible, as well as tangible.10

Brandeis and Warren’s explanation is broad and cannot possibly encapsulate everything the right to privacy has come to stand for, such as data, metadata, and the various levels of intellectual property we can obtain. I will discuss these subjects in detail as I progress.

Consider another Constitutional amendment: The Fourteenth Amendment, which says, “…nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.”11 The words of the Fourteenth Amendment are vague. However, the language of that phrase and what time has decided, is that the Fourteenth Amendment is the cornerstone to why privacy exists. The way the words “life,” “liberty,” and “property” have been interpreted stretches far beyond their primary definitions of being free to do as you like with your life and property, and being free from

11 LII/ Legal Information Institute. n.d. Fourteenth Amendment.
oppression by authority. Along with the explanation provided by Justices Brandeis and Warren above, now liberty means that you are not only free from oppression, but you have a right to never have life and property infringed upon.

The most common interpretation to the Fourteenth Amendment is that “life” means your own life and the lives you are responsible for. “Liberty” means privacy and other aspects regarding freedom of information. “Property” means everything from the house you live in to the thoughts you have. The extended definitions of life, liberty, and property may create a lot of uncertainty. What we have now is an expectation of privacy in America that, once reached, can never be reversed.

Compare privacy to offering a child a piece of pie. If you give the child a piece of pie and after a few bites you ask for it back, what are the chances that the child would give the pie back? Increase the number of children to over 300 million and every one of them were given some version of a piece of pie. Once the pie is handed out, or in this case the right to privacy, nothing can be taken back. Any object, intangible or tangible as Brandeis and Warren claimed, is fair game for litigation.

**Social Implications of Privacy**

Within the survey, I conducted in early Fall 2016, there is a question which asks “Which, if any, do you believe the government has access to on your mobile device?” with the corresponding answers of texts, call/call history, location, photos, internet search history, none of these, or all of these. Over 80% of participants answered, “all of these.” If “all of these” is the popular answer, then it seems that the general population is already fully aware of how

---

accessible their information is to the federal government. But, do we care? The question following the one above was “would you care if all of the above choices were being tracked?”\(^\text{13}\) The results were surprising, with a combined 48% of participants answering with “No, I would not care” or “I am indifferent.” 52% of participants said, “Yes, I would care.”\(^\text{14}\) These survey results were unexpected and indicate that even despite participants strongly believing their data was not solely their own, they genuinely do not care. However, quite the opposite must be true, because it is highly unlikely that 48% of people do not have something to hide. Glenn Greenwald, *The Guardian* journalist who broke the NSA story spurred by the actions of Edward Snowden says,

> I’m sure we have all heard the rationale that, ‘I’m not one of the bad people, I’m not planning a terrorist attack, so I don’t actually have anything to hide.’ Everyone has something to hide. We put locks on our bedroom and bathroom doors, we use passwords to protect our social media accounts…we understand instinctively why privacy matters.\(^\text{15}\)

Glenn attempts to explain that there are assuredly people who believe they have nothing to hide, do not mind, or are indifferent to having their information captured by the federal government. However, it doesn’t matter if you are a “bad person” or not, the right to privacy is perhaps one of our most valued, yet under-appreciated rights to ever exist.

Following the 2015 San Bernardino terrorist attack, the media was filled with stories of death and the rising threats in the United States. A crucial part of the San Bernardino investigation involved the tech company, Apple, and the Federal Bureau of Investigation (FBI). In early 2016, the FBI gained possession of the known terrorist’s Apple iPhone, however this

\(^{13}\) *Ibid.*  
\(^{14}\) *Ibid.*  
iPhone was locked and the FBI could not gain internal access. The FBI asked Apple to create a “back door” of sorts or a new software, that would allow the FBI to get into the iPhone without having to hack into it. The reason the FBI didn’t hack into it in on their own is because after 10 incorrect password attempts, all the data on the iPhone would have been erased. The issue is that Apple said no to the FBI. Apple refused to create new software simply because if the FBI succeeds in getting access to the software overriding Apple’s encryption, it would create easy access for the government in many future investigations. The situation sparked a national debate on privacy and the limits to this right.

Essentially, Apple is more worried about the reputation they have with their customers, and such a public disregard for their customer’s privacy may have negative effects on the company. Furthermore, once government entities or other companies begin asking Apple to create new software and back door access, they will never be able to reverse their actions. If Apple creates new software to open a back door, other government agencies will most likely seek orders compelling Apple to use the software to open the back door for tens of thousands of iPhones. Referencing my earlier example involving the children and the pie, once someone (Apple) does a security “favor” for someone else (FBI) then Apple will become submissive to many other requests in the future.

After reading the articles related to the Apple vs. U.S. Government fight, I can conclude that Apple was extremely cautious when it came to their customer’s privacy, both in the U.S. and abroad. Many could argue that there are vast security risks with Apple’s refusal, and they could potentially prevent another attack from happening. However, Apple believes that there should be

---

no excuses for attempting to infiltrate one phone, because in turn, millions of people’s phones and devices could potentially be infiltrated in the process.

Apple understands the expectation of privacy in America, and know that public approval of the company would dramatically decline. Millions of people in America, as well as in other countries, rely on Apple for most of their technological needs. If Apple were to succumb to the pressure of the FBI, there would be a visceral reaction from those that value their privacy the most. Perhaps the most interesting part of this fight between Apple and the FBI, is that in the end, the FBI went to a third-party hacker who could unlock the phone. The question remains, if the FBI could get into the phone all along, why even bother with the formality of getting Apple involved? Whatever the reason, a publicity stunt or otherwise, there were clearly other means by which to reach this end.

**Legal Implications of Privacy**

Following Brandeis and Warren’s interpretation of privacy in the late 19th Century and early 20th Century, it would be effective to identify cases that have continued to shape modern privacy law. First, consider the 1965 case *Griswold v. Connecticut* which concerned a married couple seeking assistance with contraception in the state of Connecticut. At the time, Connecticut had a law that prohibited any person from using “any drug, medicinal article or instrument for the purpose of preventing conception.” In a 7-2 decision, The Supreme Court struck down this law, writing that the Constitution had “penumbras” which gave this married couple an established right to privacy.

---

Without Brandeis and Warren’s breakdown of privacy rights, courts in 1962 would have had to deal with elaborate privacy cases and no precedent to decide them with. Another case to consider, *Katz v. United States*, is very similar to *Olmstead*, but was decided in favor of the plaintiff who had evidence used against him in court in the form of wiretapping that was obtained without a warrant.\(^{20}\) Almost 40 years prior, Brandeis’s dissent in *Olmstead* was upheld in the *Katz* majority. *Katz* held that a physical intrusion into a place was not necessary to violate a person’s Fourth Amendment. Justice Potter Stewart wrote, “the Fourth Amendment protects people, not places.”\(^{21}\) Stewart’s statement is a great representation of Brandeis’s understanding of the Fourth Amendment and privacy rights, because his dissent in *Olmstead* was written ahead of its time with great dispute. Then the dissent was applied to the law 40 years later with almost no dispute.

Despite these leaps in privacy law, Brandeis and Warren did acknowledge that there would be legal limitations to the right to privacy. Individual control over personal information can only stay personal until that information becomes public. Brandeis and Warren invented the right to privacy in the context of late nineteenth century America as a legal means of protecting and encouraging individual decisions whether, when, and how to share their personalities with others.\(^{22}\) Privacy law can only stretch so far until the information is no longer private. Individuals may be granted control over how to disseminate that private information should they want to make it public. However, in whatever way it does become public, willingly or not, that enters into different legal territory altogether, such as libel or tort law.

---


\(^{21}\) Ibid.

Invasion of Privacy Law

In modern Tort Law, the invasion of privacy rests in an individual’s reasonable expectation to be left alone. Therefore, an individual can also sue if they feel their privacy has been breached or their right to be left alone has been denied by a given situation or person. There are four distinct categories of the invasion of privacy Tort Law, which are (1) Intrusion Upon Seclusion, (2) Appropriation of Name or Likeness, (3) Publicity Given to Private Life, and (4) False Light. Intrusion Upon Seclusion consists solely of intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.

Appropriation of Name or Likeness is the interest of the individual in the exclusive use of his own identity, insofar as the use may be of benefit to him or to others. Publicity Given to Private Life occurs when one who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy. The matter publicized must be of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public. Finally, False Light is similar to defamation but must contain four elements that defamation does not: (1) a publication by the defendant about the plaintiff; (2) it was done with reckless disregard; (3) it places the plaintiff in a false light and (4) it would be highly offensive or embarrassing to a reasonable person.

23 Find Law. n.d. Invasion of Privacy. Thomson Reuters.
25 Ibid.
26 Ibid.
27 Ibid.
28 Ibid.
Private information going public differs from defamation because defamation is inherently false, whereas a tort of public disclosure of private facts can be true information that can do harm. An extreme example of false light is Wikileaks, an Internet site that exposes government, political, or high-profile/top clearance secrets. The information on Wikileaks is true, but is illegal most of the time because it can do great harm. The issue is that there can only be punishment if the administrator of Wikileaks was in the U.S. Since he is not, Wikileaks lives on.

The common denominator within Invasion of Privacy Law is this idea of the “reasonable person.” A reasonable person would handle their individual privacy in a certain way, and would determine how they would want their own privacy handled by others. The standard of the “reasonable man” are how the courts determine the standard to set for creating the law and deciding cases that have similar facts. Whatever an individual’s definition of a “reasonable man,” the courts have created their own and that is how one would be tried in an invasion of privacy case.

In a novel written by Dave Eggers titled *The Circle*, the main character Mae, is offered a job at the high-tech, highly social, and highly transparent company called The Circle. At this company, its employees are more open with each other about their lives and experiences than one might be with their own spouse or close family member. As Mae rises in the ranks of the company, she ultimately becomes too far gone by the overexposure and exploitation of her own life. Mae’s privacy does not exist anymore, which is essentially The Circle’s goal for their

---

employees. In very Orwellian fashion, the ongoing motto of The Circle is “secrets are lies,” “sharing is caring,” and “privacy is theft.”

The purpose of The Circle is to demonstrate that what is considered now to be a “reasonable person” is evolving, will continue to do so, and will not be bound by the same definition that it has been for over 100 years. The idea of “the circle” of privacy was arguably first explored by Erwin Chemerinsky, who says privacy is a series of circles, one surrounding the other. The inner-most circle contains the things we tell no one about ourselves or the deeply personal thoughts. The next inner-most circle contains things about us that are known only by those with whom we are more intimate, such as a spouse. The circle continues until one reaches the information that is known by all.

**Intellectual Property Law**

The term Intellectual Property (hereinafter IP) was not used commonplace until the 20th Century, even though the idea behind IP had been around since the late 19th Century. Brandeis and Warren were integral in the creation of IP because of their understanding of property in the form of “mental capital due to mental labor.” In an earlier excerpt, Brandeis said “…the law gave a remedy only for physical interference with life and property…later…the term ‘property’ has grown to comprise every form of possession—intangible, as well as tangible.” Property is no longer the foundation and walls of our homes, but “it is our thoughts and ideas—and the conceptions behind things that may become tangible in the future. Rights and protections for

---

owners of intellectual property are based on federal patent, trademark and copyright laws and state trade secret laws.”34

IP has protected individuals from essentially having their ideas “stolen” and used for purposes that may be different or the exact same as what the original individual had in mind. So, where does our data fit into the IP spectrum of protection? To answer this question, we must first look at what data is and how data can be differentiated from public information. Today, our data is everything from the texts we send and receive, to the phone calls we make. Data is our Internet browser history and the apps we buy for our mobile phones. Data is the profiles we create on social networks and the content we share on those networks. There is even an argument that our data is the entire mobile device’s operating system. Before I discuss the legal implications of data protection under Intellectual Property, I would like to properly define terms like Big Data and metadata to create a more well-rounded sense of the topic.

Big Data is an all-encompassing term for any collection of data sets so large and complex that it becomes difficult to process using on-hand data management tools or traditional data processing applications.35 This textbook definition is extremely technical. All it means is that there are everyday “items” (i.e. texts, calls) that can no longer be put into analog storage, such as on a shelf, in a drawer, or even in a removable flash drive. Instead, data must be put into some larger system that has the capabilities to store such immense amounts of digital information. Big Data is our digital makeup and where we can find it.

If we were to break down the components of Big Data even further, we would find a term called “metadata.” If Big Data is hard to understand, then metadata is an enigma. In short,

34 Ibid. AIPLA.
metadata is data that serves to provide context or additional information about other data. Some examples of metadata are information about the title, subject, author, typeface, enhancements, and size of the data file of a document. Metadata may also describe the conditions under which the data stored in a database was acquired, its accuracy, date, time, method of compilation and processing, etc.\textsuperscript{36} Elaborating a bit more on the definitions and Big Data and metadata will aid in gaining a clearer idea of just how complicated protecting these miniscule bits of information really is.

There are still very many issues that have yet to be tackled in the realm of data as property. IP is most valid in businesses, typically because businesses must hold and store a massive amount of data in their systems. For businesses and large databases, courts applied \textit{sui generis}, meaning “of its own kind” to most of these large databases because these databases were copyrightable.\textsuperscript{37} While this \textit{sui generis} system may work for now and for a certain caliber of business, the system could create an exclusive property rights regime that would be subject to few, if any, public policy limitations. It would convert existing barriers to entry into impossible legal barriers to entry.\textsuperscript{38}

\textit{Sui generis} would make it more difficult for businesses to have their intellectual property protected if their competition’s data “was there first.” Businesses are granted the same laws as individuals, since businesses are technically considered “people,” so this presents even more complications in court. Up until less than a decade ago, individuals did not even know intellectual property rights existed for themselves. In the age of data, intellectual property rights


\textsuperscript{38} \textit{Ibid}. 
have become more prevalent due to the rise in modern technology. Within the world of social media, some believe that one’s “digital self” can be harmed.

During the panel that the University of Arizona’s College of SBS hosted called Conversation on Privacy, guest speakers Edward Snowden, Glenn Greenwald, Noam Chomsky, and moderator Nuala O’Connor discuss the “digital self.” Nuala O’Connor, who is the Founder and CEO of Center of Democracy and Technology, believes in the digital self—that your data is an extension of your person, an extension of self, and should be treated as part of the body.39 O’Connor chose not to elaborate much about data as an extension of your person, so I explored the question, can someone harm your data or metadata?

Data breach harm cases typically arise in one of these three ways: (1) The exposure of their data has caused them emotional distress, (2) the exposure of their data has subjected them to an increased risk of harm from identity theft, fraud, or other injury, or (3) the exposure of their data has resulted in their having to expend time and money to prevent future fraud. Courts do not often decide in favor of these arguments because emotional damages are much more difficult to measure than physical torts are.40 If our data is an extension of ourselves and property that we own, another possible rule of law that may be applied is trespass to chattels. Trespass to chattels is any impermissible movement or physical disturbance of your property, that in turn may cause harm. Therefore, if one’s data is moved via the Internet or to various servers, then some say data undeniably qualifies as property that could potentially be trespassed upon.

There is plenty of backlash with the idea that the tort of trespass to chattels should be expanded. Some critics worry that extending trespass to chattels would stifle free speech on the

---

40 Solove, Daniel. 2014. Privacy and Data Security Violations: What's the Harm?
internet because any unwelcome email might constitute a trespass. Creating this stifle would presumably reduce people's willingness to communicate freely on the Internet and curtail the Internet's ability to function as an open, democratic forum.\(^4^1\) The Internet was not created to be a “safe” space for all of one’s valuable information to be stored. The general populous knows that your information is expendable online, and can be accessed, seen, and moved, which is why we should exercise the utmost caution when using our digital selves. For now, protecting people’s “digital selves” is not one of the court’s most pressing issues.

*We all know the world is too big for us to be significant. So all we have is the hope of being seen, or heard, even for a moment.*\(^4^2\)

—The Circle

**Modern State Surveillance**

Most of us are unaware of just how much we are being seen and heard. Despite the measures that are taken to encrypt and protect the data that we put online, sometimes it seems that virtually nothing can be hidden by government agencies, such as the National Security Agency (hereinafter NSA). Data collection may carry some weight with the courts in the future as 21st Century privacy issues progress. However, as of now data collection in the name of national security seems to be a perfectly plausible justification to the courts.

We have clearly determined that there is an expectation of privacy in the world today. However, the more research I do, the more I find that this expectation comes with people struggling to keep that right. Various aspects of privacy are slowly and subtly being taken away,

\(^4^1\) *Hamidi v. Intel Corp.* 2003. 30 Cal. 4th 1342

whether we want to acknowledge this or not. There is a lot we don’t know or understand when it comes to surveillance, and the benefits of being surveilled are equivalent to the drawbacks.

Herein lies a simple fact: we are being watched and global surveillance has never been higher. The United Kingdom has the largest percentage of surveillance in the world, using a system called “The Ring of Steel,” holding nearly half a million surveillance cameras and license plate readers in the city of London alone. The United States and Russia follow close behind. New York City has 4,000 cameras just south of Canal Street in Lower Manhattan; this is a minute area of the entire city. The strongest justification for as much surveillance as we see (or don’t see) today is that it is used to prevent and solve crimes.

This seems reasonable, right? Unfortunately, in London only one crime was solved for every 1,000 cameras in 2008, and even less so were actually prevented. The FBI has acknowledged that surveillance cameras are not the end-all solution, but they are merely in place to aid law enforcement in solving crimes and terrorist attacks, and to weed out useless information faster than any human could. Surveillance cameras are not the only means by the government to maintain a watchful eye. As made abundantly clear in the last few years, data and metadata collection is not a process that is slowing down—it is just beginning.

The NSA was created in 1952 during the Truman administration, after attempts by the government to heighten national security. Following World War II and the failed attempts by other agencies, the NSA was formed with many improvements. Its first notable use was during the Vietnam War when NSA programs could intercept phone communications of anti-war actors.

---

44 Ibid.
45 Ibid.
46 Ibid.
and civil rights leaders.\textsuperscript{47} During the War on Terror and concurrent rise of the Internet, cellphones, and other modern technology, the NSA played a large role in the first collections of what we know today as data. The NSA has received help from private entities like AT&T and Verizon to collect more accurate records of phone and Internet activity.

Edward Snowden’s leaks of NSA data collection in 2013 created a new demand of transparency by the American people at large. However, the use of transparency can go both ways. On one hand, many Americans want transparency from the American government in their general surveillance activity. On the other hand, a transparent state requires transparency from both the government and the people—leading the U.S. populous to have little to no privacy at all. The tradeoff is more complex than simply saying, “I am an American with privacy rights, therefore the government should stay out of my business…but while you’re at it, show me everything you’ve collected on me.”

The justification for national security has been heard repeatedly, and continues to be upheld in lawsuits on that basis alone. Noam Chomsky, a well-known social activist, social critic, and philosopher believes that there are different types of security. There is security for state power, which is highly protected. There is security for concentrations of economic power, or corporate interests. And there is security of the population, which turns out to be a very low consideration of very little significance that is constantly ignored or overruled.\textsuperscript{48} While Chomsky has very radical personal and political beliefs about the government’s role in society, he makes a much less radical point above.

\textsuperscript{47} Pilkington, Ed. 2013. \textit{Declassified NSA files show agency spied on Muhammad Ali and MLK.} The Guardian.

He asks how an individual can have a reasonable expectation of privacy if the individual is not afforded the same level of security that the government has. Part of Edward Snowden’s efforts to reveal information about government “spying” included the PRISM program, a massive domestic surveillance program, which uses at least 9 major internet companies to collect internet communications. How can individuals combat not only one massive government security agency’s surveillance, but that of multi-billion-dollar internet companies as well? The simple answer is that, realistically, the government receives more security because they handle the most sensitive and confidential material, which most Americans would agree with.

Laws of Surveillance

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act was created in 2001 following the 9/11 Attacks. In short, the Act gives the federal government agencies like the NSA, CIA, and FBI, a much broader set of regulations in their efforts to obtain information related to global and domestic terrorism. The PATRIOT Act also increased penalties and sentences for those who commit national security crimes, and updated the laws to reflect new and current technologies that could aid threats. Much of the justification for data and information collection is due in part to this law.

The Foreign Intelligence Security Court (FISC) oversees the legality of laws such as the PATRIOT Act and other foreign surveillance-targeted programs. The FISC can issue warrants

---


for foreign actors and provide oversight to global and domestic surveillance programs in the
NSA. The FISC has quietly become almost a parallel Supreme Court, serving as the ultimate
arbiter on surveillance issues. The FISC deliver opinions that will most likely shape intelligence
practices for years to come. Unlike the Supreme Court, the Foreign Intelligence Supreme Court
hears from only one side in the case—the government—and its findings are almost never made
public.\textsuperscript{51}

The FISC has its limits. The chief judge of the Foreign Intelligence Surveillance
Court said the court lacks the tools to independently verify how often the government’s
surveillance breaks the court’s rules that aim to protect Americans’ privacy.\textsuperscript{52} Even the court that
was assigned to give oversight to national and international security programs in the first place,
often doesn’t receive adequate access to information from these agencies. Under many of the
broad and ambiguous pieces of legislation, such as the PATRIOT Act and the PRISM program,
surveillance is perfectly legal.

\textit{Surveillance in Theory}

The fact that we are allegedly “being watched” is not a new concept. Living in a state of
surveillance has been weaved in and out of most of the world’s nations and societies over time.
In 1791, English philosopher Jeremy Bentham designed The Panopticon prison. The prison is
described as a circular building, with the prisoners’ cells arranged around the outer wall and the
central point dominated by an inspection tower. From this building, the prison's inspector could

\textsuperscript{52} Leonnig, Carol D. 2013. \textit{Court: Ability to police U.S. spying program limited.} The Washington Post.
view the cells at any time, though the inmates themselves would never be able to see the inspector himself. Assuming that the omnipotent inspector was always watching them, prisoners would modify their behavior and work hard, in order to avoid punishment.\footnote{UCL Bentham Project. n.d. \textit{The Panopticon}. University College London.} The Panopticon is a physical manifestation of the type of surveillance we have now or may see in the future.

The goal of Bentham’s Panopticon is to correct people’s behavior over time. Eventually, the behavior will be so habitual, that the “inmates” aren’t phased by the fact that they might be watched, because they have nothing to worry about. This should sound familiar, given the old “if you have nothing to hide, you have nothing to fear” logic. Jake Goldenfein from the University of Melbourne says, “the relevance of The Panopticon as a metaphor begins to wither when we start thinking about whether contemporary types of visuality (effectively digital and data-driven) are analogous to the central tower concept.

In The Panopticon, the occupants are constantly aware of the threat of being watched—this is the whole point—but state surveillance on the internet is invisible. There is no looming tower and no dead-eye lens staring at you every time you enter a URL.”\footnote{McMullan, Thomas. 2015. \textit{What does The Panopticon mean in the age of digital surveillance?} The Guardian.} For the most part we are all aware that someone could be watching or tracking our digital activity. However, the rationale should not be that we have nothing to hide and therefore nothing to fear. Instead, we shouldn’t be “watched” in the first place, because our most basic human rights grant us protection from the watching itself. For some, the national security interests in America are all it takes to be convinced that being surveilled in OK. To that I say, national security may be at stake, but should national security include trampling on the protections in place to reach an obscure goal? What is national security without a loyal and trusting populous?
The further we depart from actually believing in our own government, the closer the government will get to intrusion upon our homes, our property, and our data. George Orwell’s chilling dystopian novel, *1984*, is a stark reminder that a transparent state where the government is close to our everyday lives may already be in practice in a much less obvious way. In the novel, the extreme surveillance methods are exemplified in the “telescreens” where someone can quite literally watch a person in their home. *1984* is one of the more intense examples that may be applied to the point I am attempting to make, but *1984* was never intended to make us scared of our government, or make us paranoid and distrustful of all authority. Instead, Orwell believed that in order to make our causes better, there must be constant criticism of the system in which we live. To prevent a world of totalitarianism, we must remain vigilant of the higher authority that governs us and hold fast that the authority must carry the burden of proof, rather than the people.

**Conclusion**

American laws seem to be very straightforward at first glance. We are overseen by a document that lays out rules and limitations for our government to follow. However, there is a lot of confusion for some of the rights that we have in the modern lives we all now live. Privacy is one of these rights. Privacy has been defined, redefined, and scraped to its core by many scholars and Supreme Court justices. The right to privacy and its boundaries in the 20th Century were expressly demarcated. In the age of data and technology, privacy is becoming more obscure because we are unaware of how to approach it. Is there an expectation of privacy in America today that encompasses everything we want kept private?

---

Presented here was a comprehensive history of where we have seen our right to privacy applied, where it came from, and who has talked about it. Justice’s Louis Brandeis and Samuel Warren have spoken in detail about what our right to privacy means and where the burden of proof rests in keeping this right. Since American property rights are well-defined, I wanted to explore the idea that data and metadata can be considered property in a modern context.

Since data is part of the “selves” that we create, it is highly likely that the data we share, and store on our tech devices can be protected from infringement. This protection may not be a reality anytime soon since the courts are still attempting to define the modern version of property and “the self.” After explaining the social and legal implications of privacy in America, as well as the intellectual property and invasion of privacy law in place, I discussed surveillance and how “watched” we really are.

The breadth of this topic is enormous, and there is no realistic way to ask and answer every question or idea posed. Brandeis and Warren spent eleven pages alone, simply discussing what privacy is. The goal set forth as I began typing was to shed light on the importance of our rights in America, and specifically our right to privacy in the age of modern technology. I am a firm believer in maximal liberty for the citizens of this great nation. I do not believe this liberty can be achieved without a comprehensive knowledge of the rights that we have. My hope is that these pages are informal enough to read and yet give a smart and direct account of one of the most fundamental, and often ignored, rights we have today.

**Research Question**

Only some questions can be truly answered in exploring a topic such as this one. The beauty of probing this topic is that much of the content and many of the questions have yet to be
researched to an extent adequate enough to provide concrete answers, which leaves a lot of room for exploration. One of the larger questions that has framed my research and will further frame this paper is, what does American Law say about privacy, property in the form of data, and our current state of surveillance?

**Scope of the Study**

In my own research, I took to a broad and cumulative survey regarding privacy in America and what we seem to know, or not know, about it. This survey reached 57 people and was administered via word-of-mouth, social media, and people in my general area at a given time. 70.2% of participants were between the ages of 17-25, with 29.8% aged 26 and over. From these results it is very clear that the primary age group targeted was college-aged students or those recently graduated, which framed the bulk of my survey findings with a young, millennial point of view.

The aim of my Thesis was not to capture results from certain people, but instead to use these results as a very small sample of how people think about the rights we have in America today. The goal of the survey was not to analyze answers to specific questions, but rather to gain an understanding of how much we care about current events and if we are able to identify occurrences in these events where the legality may be questioned. My objective with the survey study and other research was to hopefully open the eyes of those who may never have thought about the right to privacy as an actual issue.
Bibliography


Harvard Law Review.


College of Social and Behavioral Sciences.

Department of Justice. n.d. The USA PATRIOT Act: Preserving Life and Liberty. Department of Justice.


Find Law. n.d. Invasion of Privacy. Thomson Reuters.


Hamidi v. Intel Corp. 2003. 30 Cal. 4th 1342


Kelly, Heather. 2013. After Boston: The Pros and Cons of Surveillance Cameras. CNN.


LII/ Legal Information Institute. n.d. *Fourteenth Amendment.*

—. n.d. *Fourth Amendment.*


*Olmstead v. United States.* 1928. 277 U.S. 438


http://thelawdictionary.org/privacy/.

Visual Survey Results

Figure 1

What, if any, do you believe the government has access to on your mobile device?
(57 responses)

- Texts: 9 (16.8%)
- Calls/Call History: 11 (19.3%)
- Location: 15 (26.3%)
- Photos: 5 (8.8%)
- Internet Search History: 10 (17.5%)
- All of these: 48 (80.7%)
- None of these: 0 (0%)

Figure 2

Would you care if all of the choices above were tracked? (i.e. texts, calls...)
(57 responses)

- Yes, I would care: 38.6%
- No, I would not care: 8.8%
- I am indifferent: 52.8%
Figure 3

Is it legal or illegal for the choices above to be tracked? (57 responses)

![Pie chart showing percentages of responses]

Figure 4

What are the 5 basic freedoms guaranteed by the 1st Amendment in the United States Constitution?

(57 responses)

<table>
<thead>
<tr>
<th>Freedom</th>
<th>Percentage</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Religion</td>
<td>55 (96.5%)</td>
<td>55</td>
</tr>
<tr>
<td>Press</td>
<td>56 (98.2%)</td>
<td>56</td>
</tr>
<tr>
<td>Speech</td>
<td>47 (82.5%)</td>
<td>47</td>
</tr>
<tr>
<td>Privacy</td>
<td>6 (10.5%)</td>
<td>6</td>
</tr>
<tr>
<td>Life</td>
<td>10 (17.5%)</td>
<td>10</td>
</tr>
<tr>
<td>Assembly</td>
<td>49 (86%)</td>
<td>49</td>
</tr>
<tr>
<td>Liberty</td>
<td>22 (38.8%)</td>
<td>22</td>
</tr>
<tr>
<td>Petition</td>
<td>35 (61.4%)</td>
<td>35</td>
</tr>
<tr>
<td>None of these</td>
<td>0 (0%)</td>
<td>0</td>
</tr>
</tbody>
</table>