Nothing to Hide: The Development of American Privacy Law and the Fourth Amendment

Cole A. Cadman

Department of Government and Justice Studies, Appalachian State University

Honors Thesis

April 21, 2019

Approved by:

Marian Williams

Marian Williams, Ph.D., Thesis Director

Kathryn Montalbano

Kathryn Montalbano, Ph.D., Second Reader

Ellen Key

Ellen Key, Ph.D., Departmental Honors Director

Jefford Vahlbusch, Ph.D., Dean, The Honors College

Abstract

Technology has always presented itself as a problem for the court system. As the pace of technological development increases over time, this problem will only worsen. The current operating standards of privacy law in relation to technology is outdated and in need of a thorough review. This thesis examines Supreme Court cases that established a constitutional right to privacy as well as Supreme Court cases that examined how that constitutional right is interpreted depending on several different technologies and scenarios. After a review of Supreme Court cases, this thesis proposes three changes that seek to bring privacy law in line with current technology. Those changes are revisiting the third-party doctrine, clarifying the data collection and management process, and redefining what the public considers a reasonable expectation of privacy.

Nothing to Hide: The Development of American Privacy Law and the Fourth Amendment

Introduction

There has always been, and likely always will be, a constant struggle between privacy advocates and the American government. On the one hand, the United States government argues that, although their practices may undermine the right to privacy of their citizens, the government engages in these actions for public safety purposes. On the other hand, privacy advocates argue that, while increased privacy may interfere with public safety, the right to privacy is fundamental. While this struggle is constant, it appears that recent technological advances have made infringements of privacy more and more common. The court system has always struggled to keep up with the pace of technology. At the turn of the 20th century, inventions like the telephone were challenging the standards that the telegraph had earlier established which had challenged the norm of physical mail. Now, in the early 21st century, the court system is struggling to keep up with the pace of mobile technology. As a result, the government has capitalized on this gap, intruding on the privacy of individuals. Nothing short of a fundamental restricting of American privacy law is required to properly address the issues of privacy in the digital age.

Privacy is a fundamentally difficult concept to enshrine in law. What one person considers a private matter is highly unlikely to be the same across an entire society. For instance, some people are more than comfortable being open and honest about their sexual orientation, while others, due to societal pressures or dangers, will keep their sexual orientation a closely-guarded secret. A less extreme example is simply that some people are willing to create social media accounts where they update potential strangers about their whereabouts, likes, dislikes,

friends, and a wide variety of other personal information, while others choose to keep that information private. With all this in mind, it is difficult to find a universally accepted standard of what should or should not be considered private.

Another difficulty in establishing a standard of privacy is the combatting interests of the government and the public. Both the government and the public have legitimate interests in either chipping away, maintaining, or building privacy rights. For the government, very high standards for privacy rights make the job of ensuring public safety more difficult as the government jumps through more legal and procedural hoops to gather information on individuals. For the public, high standards for privacy rights makes it more difficult for the government take advantage of the public's rights, which lessens the opportunity for tyranny. A workable standard of privacy rights in the United States would find a solution that both allows the government to pursue its legitimate interests in ensuring public safety while also ensuring that, in the pursuit of those interests, the government does not exceed an acceptable standard. Of course, this is easier said than done.

While not explicitly mentioned in the Constitution, several amendments imply the right to privacy that, when taken together, paint a picture of legal privacy. The 1st Amendment contains protection for the privacy of beliefs based on the protection of religious freedoms, free speech, and free association. The 3rd Amendment, while rarely discussed, includes protection for the privacy of a person's home from quartering soldiers. Arguably the most important amendment in terms of privacy is the 4th Amendment, which prohibits unreasonable searches and seizures and requires a judge or magistrate to issue a warrant to conduct a search or seizure based on probable cause. Additionally, the 5th Amendment protects an individual's right to avoid self-incrimination, meaning there is an implicit right to privacy of personal information. That

being said, constitutional scholars express a wide range of beliefs regarding the constitutional right to privacy. Therefore, the fact that the Bill of Rights implies the right to privacy does not do much for the purpose of this work.

Although the legal definition of the right to privacy is difficult to determine, there are several clear issues that need addressing by the court system. First, mobile technology in cellphones, computers, and even cars has outpaced the ability of the court system to keep up. In the 1980s, the height of police technology was the use of beepers to track people or substances remotely. These devices were well-defined in their usages and offered little potential for abuse. Today, however, just about everyone in the United States carries with them a cellphone, which not only tracks their every moment, but communicates with just about everyone they know, browses the internet, and even access their finances. The pace at which technology progressed from beepers to near-constant access to an individual's movements, locations, beliefs, communications, and finances has been blistering. Put simply, the court system has not had enough time to adjust.

Second, the court system has not effectively adapted the standards with which it uses to judge the extent of an individual's right to privacy. The amount of data that third-party companies possess on their users is staggering. This information is what the government and police want when they are conducting surveillance against an individual as was demonstrated by the revelation of the government's PRISM program. Phone companies or Internet Service Providers are third parties and therefore it is not entirely clear whether they have the authority to give up information about a suspect nor is it clear that they can give up that information without the permission of the users. Such a discrepancy must be cleared up.

Finally, Americans need to know more about both how their personal information is being used by both companies and the government as well as ways they can be more responsible wards of their information. This thesis examines where the court system currently stands in regards to the right to privacy in a digital age as well as addresses potential ways the United States could find a balance between fulfilling government and public interests.

The Supreme Court and the Constitutional Right to Privacy

In the discussion of what the right to privacy in the United States looks like today, it is important to establish two things. The first thing to establish is whether or not the Supreme Court has verified that such a right exists and, if they have, the second thing to establish is how the Supreme Court has said such a right protects individuals from certain police actions. There are a number of Supreme Court cases which addressed with whether or not a right to privacy exists and going over every single one of them would be overly exhaustive. Therefore, this thesis will only examine major cases, as they provide a clear enough picture of what the Supreme Court has said.

The Court has said that there are a variety of instances in which an individual's right to privacy can serve as the basis of protection from state actions. These have varied greatly over time but when viewed together, the decisions can serve to create a picture of privacy according to the Supreme Court. In *NAACP v. Alabama* (1958), the Court held that Alabama's attempt to subpoena the National Association for the Advancement of Colored People (NAACP) for a membership list was unconstitutional. Justice Harlan noted that the Court "recognized the vital relationship between freedom to associate and privacy in one's associations" (*NAACP v. Alabama,* 1958, p. 462). In other words, the freedom of association also carries with it the right to privacy in whom one associates with.

Griswold v. Connecticut (1965) established that a Connecticut law prohibiting the use of contraceptives by married couples was an unconstitutional breach of a couple's right to privacy. Justice Douglas wrote, "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" and, "The present case, then, concerns a relationship lying within the zone of privacy created by several fundamental constitutional guarantees" (*Griswold v. Connecticut,* 1965, p. 485). In other words, by examining earlier Court decisions and by a close reading of the Bill of Rights, the majority had decided that a constitutional right to privacy was implied. The Court would also later extend the right to unmarried couples in *Eisenstadt v. Baird* (1972). In this instance, the Court recognized that the right to use contraceptives was based on the right to privacy in marriage and relationships.

The *Griswold* decision preceded an even more controversial decision, *Roe v. Wade* (1973), in which the Court recognized that the constitutional right to privacy protected a woman's right to seek an abortion. *Roe*, like *Griswold*, said the right to privacy was found in the penumbras of the Bill of Rights, meaning that it is suggested, not stated. *Roe* also drew on earlier cases, such as *Meyer v. Nebraska* (1923) and *Pierce v. Society of Sisters* (1925), which dealt with parental rights to educate their children as they saw fit, suggesting a right to privacy in education.

Lawrence v. Texas (2003) further established that a right to privacy exists by striking down a Texas law that prohibited same-sex sexual contact. Citing *Planned Parenthood v. Casey* (1992), Justice Kennedy states, "our laws and tradition afford constitutional protection to personal decisions relating to marriage, procreation, contraception, family relationships, child rearing, and education" (*Lawrence v. Texas*, 2003, p. 574). Because of these and several other reasons, the Court reversed the decision of *Bowers v. Hardwick* (1986).

The Supreme Court recognizes that a constitutional right to privacy exists, even though it is not explicitly mentioned in the Constitution. This right is not absolute, however, as the Justices note in just about every case in which privacy is mentioned. This area in which it is unclear whether or not the right to privacy is involved is where the controversies that exist today are born from. What follows will be a review of Court cases pertaining to police and technology in which privacy is a central concern.

Privacy from Police Action

The Fourth Amendment came out of, among other things, the Framer's disapproval of the use of general warrants by the British. In short, a general warrant effectively allowed police officers to conduct a search of anyplace they wanted with little to no oversight whatsoever. With this memory fresh in their minds, the Framers wrote the Fourth Amendment expressly intending to curtail the ability of police to conduct searches and seizures without oversight and approval. With that said, the Supreme Court has dealt with many cases involving privacy from police action and what follows is a discussion of several of the most important cases which have come before the Supreme Court.

In *Olmstead v. United States* (1928), Roy Olmstead was suspected of conducting illegal bootlegging. In their surveillance and without a warrant, prohibition agents set up wiretaps on several homes and an office in which they suspected Olmstead was conducting business related to the bootlegging. After several months of surveillance, the agents arrested Olmstead. Olmstead challenged the arrest on the basis that his Fourth Amendment rights were violated because the agents had collected information on him without a warrant. Writing for the majority, Chief Justice Taft said that because there was no physical intrusion into a constitutionally protected area and that because there was no seizure of physical evidence the listening in on conversations

did not qualify as evidence under the Fourth Amendment: there was no search and seizure and, therefore, no warrant was required.

In his dissent, Justice Brandeis noted, “Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world” (*Olmstead v. United States*, 1928, p. 472). In other words, although the collection of conversations through the use of a wiretap may not be a literal seizure of physical evidence as Chief Justice Taft claims was necessary to constitute a search and seizure, the Constitution ought to be read with the understanding the Framers could not have foreseen such advancements in technology as the Justices were dealing with in this case.

Further, Justice Brandeis notes, “The mail is a public service furnished by the Government. The telephone is a public service furnished by its authority. There is, in essence, no difference between the sealed letter and the private telephone message” (*Olmstead v. United States*, 1928, p. 475). Government agents are required to secure a warrant before they may search and seize a suspect’s mail. As Justice Brandeis points out, the conversations a person has through the phone carries with it the same expectation of privacy. Such an understanding of privacy, however, would not be realized until a later Supreme Court case which will be discussed here. That being said, Justice Brandeis’ dissent laid the groundwork for discussions of privacy law that are still being had today.

Katz v. United States (1967) was the culmination of several cases spanning the first half of the 20th century that dealt with how advancing technology was enabling police to be more and more effective at gathering information on suspects. Earlier cases had held that the use of technology to collect information about suspects without a warrant, usually involving a wiretap or microphone, would only be considered unconstitutional so long as there was some kind of

physical intrusion into a constitutionally protected area like a home (*Olmstead v. US* 1928; *Goldman v. US* 1942). *Katz*, however, would change this standard dramatically and lead to the Court adopting a new standard for determining whether or not a search violates the Fourth Amendment.

In *Katz*, Charles Katz was arrested on charges related to gambling based on evidence gained by placing a listening device on the outside of a public phone booth without a warrant. Katz argued that such a search violated the Fourth Amendment but, because precedent required a physical intrusion to have taken place, lower courts upheld his conviction. The Supreme Court did away with the physical intrusion standard on the basis that "the Fourth Amendment protects people, not places." (*Katz v. US,* 1967, p. 351) While the Court noted that it was likely that the police would have received a warrant if they had applied for one, as their search was conducted narrowly and with high amounts of care to ensure that only Katz was surveilled, their failure to do so was ultimately detrimental to their case.

An important note to remember is the issue of warrants. In most cases that deal with potential infringements of the right to privacy, it boils down to whether a warrant is required. The question is, usually, not whether the act is a violation on its face. So, it is important to remember that any proposed changes will mostly concern how police interact with the public in regards to whether they are required to obtain a warrant before conducting a search and seizure or if a certain technology allows for an exception to the warrant requirement.

Justice Harlan, in his concurrence with the majority opinion, laid out the standard by which future cases would determine the validity of a search, with his "reasonable expectation of privacy." Harlan noted that, in order to meet the standard, it was necessary to prove that "a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, that the

expectation be one that society is prepared to recognize as "reasonable."" (*Katz v. US,* 1967, p. 361) In this case, because Katz had closed the door to the telephone booth and paid the price to use the phone, he had demonstrated that he expected his conversation to be private and the general public would agree that the conversation held inside a phone booth is not intended to be heard by the general public.

While *Katz* is a landmark decision that made large steps towards bringing the protections of the Fourth Amendment in alignment with the development of technology, questions still remain. Can the standard of a reasonable expectation of privacy be refined further? What one person considers private is unlikely to be the same as another and the invention of the internet and mobile phones has completely changed the privacy landscape. How does a person demonstrate an expectation of privacy on the internet? How does a person demonstrate an expectation of privacy if they are carrying their mobile phone with them? How does the fact that phone companies and internet service providers operate as third parties come into play? While some of these questions will be addressed here, some are still up for discussion.

In demonstrating an expectation of privacy when using technology and the internet, people do have some limited options. Services like DuckDuckGo or ProtonMail offer an alternative to Google and Gmail and are marketed for their focus on the privacy of their users. It would follow, then, that a person choosing to use those services rather than the mainstream services are exhibiting at least some form of an expectation of privacy. Furthermore, there is much discussion revolving around how a person walking in public has little to no expectation of privacy as they can be easily seen by those around them. However, can a person truly say that they remember every single person they interacted with in a day, especially if they are only passing by a person on the street? It seems like a stretch of the imagination to argue that people

have little to no expectation of privacy in public considering the fact that most of the people they see in a day are strangers and the moments they interact with them are limited at best.

The Third-Party Doctrine

The third-party doctrine is the legal practice of operating under the assumption that the information a person willingly provides to a third party like a bank or Internet Service Provider is not subject to the reasonable expectation of privacy standard established by *Katz v. United States* (1967). This means that the police could obtain information from third parties without the use of a warrant. This practice was established by two cases: *United States v. Miller* (1976) and *Smith v. Maryland* (1979).

In *United States v. Miller*, Mitch Miller was suspected of operating an illegal distillery. In order to prove his connection to a distillery, the Alcohol, Tobacco and Firearms Bureau (ATF) subpoenaed Miller's bank for all of Miller's documents. The bank then provided these documents without notifying Miller. The documents linked Miller to the distillery equipment and Miller was charged. Miller would then challenge the use of the bank documents in court, saying the bank had no authority to give that information to the government without a warrant.

The Supreme Court, however, ruled that the information the bank gave to the ATF was not protected by the *Katz* standard of a reasonable expectation of privacy. Writing for the majority, Justice Powell noted, "All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." (*United States v. Miller,* 1976, p. 443) In other words, the information that was subpoenaed was information that Miller should have known would not be privately dealt with and because the bank was a third party, the bank could hand over documents without a warrant.

This practice, known as the third-party doctrine, expanded in *Smith v. Maryland*. The circumstances of *Smith* were similar to that of *Miller*, except in this case, the third party was a telephone company who used a pen register, at the request of the police, to keep track of the numbers Michael Smith called. The Court ruled that there is no reasonable expectation of privacy for the numbers a person calls because it is general knowledge that telephone companies need to know what phone numbers are being reached in order to place calls. Especially important for this case was that the content of conversations was not monitored.

In a dissenting opinion, Justice Marshall noted, "Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes." (*Smith v. Maryland,* 1979, p. 749) Justice Marshall also wrote, "Implicit in the concept of assumption of risk is some notion of choice...By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance." (*Smith v. Maryland,* 1979, p. 750) This dissent is one of the bases of concerns still in place today. In fact, the concerns that Justice Marshall raised in 1979 have grown more relevant over the years as the amount of information that technology collects has grown, and an understanding of how it does this collection has diminished. Additionally, as the use of technology has grown more pervasive, choosing not to use technology to in order to avoid invasion of privacy has grown more difficult.

The third-party doctrine has largely stood the test of time. That being said, the Supreme Court ruled in *Carpenter v. United States* (2018) that the third-party doctrine could not be extended to the collection of cell site location information. This means that, in order to access cellphone location records, police are now required to obtain a warrant. The reason for this decision not to extend the third-party doctrine hinged on the fact that cell phone information is

far more invasive than bank records or phone numbers. While a pen register can only show what numbers a person dials and reaches, cell site location information provides near perfect data about where a person was. Considering that the use of cell phones has become effectively universal, this would grant the ability to collect large amounts of information without the use of a warrant had the Court not declined to extend the third-party doctrine here.

An earlier case, *Riley v. California* (2014), dealt with whether or not police could search through the digital information on a phone without a warrant after having arrested someone. Riley, a gang member, was arrested after being pulled over for expired tags. A search of the car revealed concealed weaponry. The arresting officer, suspecting Riley of being a gang member based on items found in the car, accessed his phone and found more evidence that Riley was involved in gang activity. After arriving at the police station, another officer found further evidence. The search conducted on Riley's phone was ultimately ruled unconstitutional, as the search did nothing to ensure the safety of the officers who arrested Riley and the search was conducted without a warrant. Writing for the majority, Chief Justice Roberts wrote, "Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one." (*Riley v. California,* 2014, p. 2486)

In general, the third-party doctrine means that the government has wide authority to request information from third parties about suspects without the need for a warrant. That being said, as the information available to third parties has grown exponentially, the Court is signaling there may be more change coming in the future as third parties now cannot surrender cell site location information without a warrant. Further, information from a cell phone gained after an arrest requires a warrant to be used in court.

Location Tracking

Having established how police and the government may interact with third parties regarding warrantless searches of technology and other records, it will be useful to examine another area of interest: location tracking. Police have long had the right to visually surveille suspects at their homes, places of work, and in their travels subject to some restrictions. However, technology such as GPS, drones, and cell-site location information tracking has the potential to make surveillance of suspects far easier and more efficient. This enhancement of abilities is what is of the most concern and debate.

United States v. Knotts (1983) dealt with the warrantless placement of an electronic device called a beeper in a shipment of chloroform in order to track suspects over a short distance. The police then used the beeper, alongside using visual surveillance, to follow the vehicle containing the shipment of chloroform to a cabin owned by Knotts that was being used to manufacture drugs. Justice Rehnquist wrote on the behalf of the Court that, "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" (*United States v. Knotts,* 1983, p. 282) and "Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case." (*United States v. Knotts,* 1983, p. 283)

Because the use of the beeper was narrowly tailored to support visual surveillance of a suspect and did not reveal any information about what was going on at the private property of the cabin aside from the delivery of chloroform, the Court ruled that the warrantless placement of the beeper in the shipment of chloroform was not a violation of the Fourth Amendment. Additionally, although the beeper allowed police to find the cabin after visual surveillance lost

the truck carrying the shipment of chloroform, the beeper only made what was already possible with visual surveillance happen sooner. Thus, the Court ruled in the police's favor. The Court also claimed that should there be abuse of this standard of practice, there will be ample time to reassess our practices as technology develops (*United States v. Knotts,* 1983, p. 284).

The *Knotts* decision was expanded in *United States v. Karo* (1984), when the use of a beeper revealed information that could not have been gained by visual surveillance. In *Karo,* a suspected drug trafficker was monitored via a beeper placed in what he believed was a can of ether. While the Court ruled that the placement of the beeper was still not a violation of the Fourth Amendment, the monitoring that police did ultimately violated the Fourth Amendment. While in *Knotts* the use of the beeper ended before the beeper was inside private property, the beeper in *Karo* was used while the can of ether was inside private property. This allowed police to locate it without the use of visual surveillance.

Writing for the majority, Justice White noted, "The monitoring of an electronic device such as a beeper is, of course, less intrusive than a full-scale search, but it does reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant." (*United States v. Karo,* 1984, p. 715) Importantly, the Court did not argue that the placement of the beeper violated the Fourth Amendment as it was placed with the consent of the then-owner. Instead, the Fourth Amendment was violated only when the beeper was used while the container was on private property.

The key, it seems, for cases involving technology and infringement of privacy is whether or not the technology enhances the senses of police in such a way as to make possible something they could not have done without the technology. The police and government do have more authority to conduct wiretaps or other forms of surveillance than does the public. So, the

reasonable expectation of privacy that an individual has is different in the contexts of another member of the public versus a police officer or government official. Additionally, it is important to note that the Supreme Court is not saying that police cannot engage in this kind of behavior. Instead, the Supreme Court is saying that police need to obtain a warrant before they engage in this kind of behavior.

Suffice it to say, technology has advanced since the time of electronic beepers. The use of a Global Positioning System (GPS) device makes it possible for police or the government to know exactly where a person is, was, and in some cases will be. Furthermore, the overwhelming majority of people now carry a device with them at all times, their cell phone, which has GPS capabilities and can track them without their knowledge. While *Carpenter* dealt with an aspect of locating based on cell phones, the Supreme Court has also ruled on the placement of a physical GPS device on a vehicle in *United States v. Jones* (2012).

Antoine Jones was suspected of drug trafficking and, after receiving a warrant, police placed a GPS device on Jones' car. However, the warrant required that the device be placed within ten days of the issuing of the warrant and that it be placed while the car was in the District of Columbia. Not only did police not place the device until eleven days after the issuing of the warrant, but they also placed the device on the car while it was in Maryland. The Supreme Court ruled that the placement of the device on the car and its monitoring constituted a search and seizure.

Writing for the majority, Justice Scalia made the claim that, although *Katz* expanded the Court's understanding of the Fourth Amendment to include instances other than physical intrusion, it did not rule out the use of the physical intrusion standard in later cases. Here, Scalia argues, unlike *Knotts* and *Karo*, the GPS device was placed on Jones' property and the search

and seizure began after the warrant had expired, meaning that the search and seizure were done effectively without a warrant according to the law. Therefore, the Fourth Amendment had been violated (*United States v. Jones* 2012).

What can be learned from *Jones* is that the placement of a device on a car constitutes a Fourth Amendment search. However, there is still much that is not known. Many modern cars have GPS already installed by the manufacturer. Can the police or the government use the third-party doctrine to subpoena that information from the manufacturer? Or could they avoid that altogether and track the car based on its communication with satellites? These questions remain unanswered. Considering how the Court has ruled in *Jones*, however, it would seem to be that using a GPS device that has already been installed on a car does not change the protections that a person enjoys from GPS tracking. Most cars that are being produced now are coming with pre-built GPS systems without the express consent or even knowledge of the complexity of the systems of the buyers. Because consent is a grey area in terms of expectations of privacy and assumption of risk, this is likely to be a major issue in the near future.

Enhanced Senses

Finally, there is the issue of how technology can enhance the police's ability to visually see things. While beepers and GPS allow the police to track objects even if they cannot see them with their eyes, they cannot see through walls or over fences. But, as technology advances, the ability of the police to do just that advances as well. What follows is a brief discussion of several cases in which this issue was raised.

In *California v Ciraolo* (1986), the police used aerial surveillance over the home of Ciraolo to see that he was growing marijuana. This surveillance was conducted based on an anonymous tip and was conducted without a warrant. After seeing the marijuana from the sky,

police obtained a warrant to search the home and arrested Ciraolo. Important to note here is that Ciraolo had constructed a fence around his home, indicating that he had an expectation of privacy, at least from the street level. What was in question was whether or not the warrantless search by police in the air was a violation of the Fourth Amendment.

Writing for the majority, Chief Justice Burger said that, although Ciraolo had established an expectation of privacy for himself by putting up a fence, "Whether respondent therefore manifested a subjective expectation of privacy from *all* observations of his backyard, or whether instead he manifested merely a hope that no one would observe his unlawful gardening pursuits, is not entirely clear in these circumstances." (*Ciraolo v. California,* 1986, p. 212) Burger notes, specifically, that a person could see over the fence if they were on top of a truck. So, while Ciraolo had established an expectation of privacy for himself, the Court did not believe it would be accepted by society.

Where this becomes controversial in the 21st century is the invention of drones. Drones are small, cheap, and widely available devices which allow anyone who purchases one to fly at considerable heights and ranges from the controller, all while recording video and taking pictures. This makes aerial surveillance far easier than before and raises questions about how applicable *Ciraolo* may be in an age of commercial flight being possible for a fraction of the cost it requires to fly a plane or a helicopter. Currently, a number of states prohibit the use of drones by police, while other states permit their use with warrants or in exigent circumstances (e.g., search and rescue).

Lastly, there is *Kyllo v. United States* (2001), which concerns the use of a thermal imaging device to conduct surveillance on a house suspected of operating as a growing operation for marijuana. Police, without securing a warrant, used a thermal imaging device to measure heat

coming out of a house. The garage demonstrated an unusually high amount of heat and the police used this to secure a search warrant where they discovered a large amount of marijuana being grown. However, questions were raised over whether or not police could use the thermal imaging device to conduct a search without a warrant.

Justice Scalia delivered the majority opinion and said that “obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area,"...constitutes a search— at least where (as here) the technology in question is not in general public use.” (*Kyllo v. United States,* 2001, p. 34) The fact that this search involved a house is important for the case, as the protections of the home are much higher than in other places. Additionally, the distinction that the device used was not publicly available complicates matters because thermal imaging is commercially available now and as earlier mentioned in the case of drones, can be easily used by police and government.

In summary, the Supreme Court has made several rulings dealing with the Fourth Amendment, privacy, and technology. But these rulings are not keeping pace with technology as it develops. While, in the 20th century, an argument could be made that the court system had enough time to adjust as technology was invented, the speed at which new technology is being invented now means that the courts cannot keep up. Further, the standards which the court system has already established are showing their age as the questions they left unanswered are now being raised.

Proposed Changes

What Kind of Understanding of Privacy Can We Accept as Reasonable?

In determining what changes are necessary to align the law with the pace of technological development, it is necessary to establish a framework from which we may view scenarios in which privacy is an issue. McArthur (2001) proposes two principles to guide our understanding of privacy: the mischance principle and the voluntary principle. The mischance principle states that "we cannot reasonably expect to maintain privacy over that which another person could discover, overhear, or come to know without concerted effort on his/her part to obtain this information" (McArthur, 2001, p.124). As an example, McArthur notes that a person undressing in front of a window without the curtains drawn cannot reasonably expect that a person walking by will not see them naked. The voluntary principle states that "if [a person] choose[s] to decrease the relative amount of privacy for [themselves] and information under [their] control by exposing it to view, [they] thereby decrease the reasonableness of any expectation that this privacy will be observed" (McArthur, 2001, p. 124-125). This principle is essentially the third-party doctrine, in that it assumes that giving information to another person means that anyone can potentially view that information.

These principles provide a good starting point but do present some problems in the context of today. For instance, McArthur (2001) believes that a reasonable person would expect to have qualified privacy when browsing the internet or using email. McArthur (2001) argues that using the internet is analogous to browsing magazines in a store with security cameras that we know are following our moves and, therefore, does not violate the mischance principle. Because we know that we are being recorded when we browse magazines in the store, we do not have a reasonable expectation of privacy in terms of what magazines we picked up. Much like

the store, McArthur (2001) argues, we know that we are being tracked when we browse the internet and, therefore, we have no reasonable expectation of privacy when we browse the internet. By comparing browsing the internet to security cameras following a person while they browse magazines, however, McArthur (2001) presents a problem with the mischance principle.

What differentiates tracking online or on the phone from security camera surveillance is the concerted effort required by the latter but not the former. In order for a store owner to know what magazines a customer browsed while they were in their store, the store owner has to seek that person out in the security footage that was recorded that day and take note of the magazines they viewed. By contrast, internet and telephonic tracking largely occurs automatically, storing the information in databases that are easily accessible by companies who can turn that information over to government agencies. The effort required by government agencies or companies to gain information about a person is reduced greatly by the internet, meaning that a person would not simply stumble upon information that is gained by internet tracking or by records kept by phone companies.

Similarly, McArthur (2001) argues that, because it is a widely known fact that email is a generally insecure form of communication, a person who sends emails that contain private information cannot then expect that information to remain confidential. In this way, email fulfills the voluntary principle in that a person is knowingly exposing their information to potential dissemination. This example is more complex than the earlier example. Considering how pervasive email has become as a means of communication, people generally do not have the option not to use email both in work and personal circumstances. For instance, a person may be required to send documents containing personal medical information to their doctor over email or they could receive credit card statements through email rather than traditional mail. While it

may have been the case that a person could have potentially gotten by without the use of email in 2001, when McArthur's piece was published, this is simply not the case today. What this means is that the voluntary principle no longer applies to things like email, as we are increasingly forced to use technology even if we know that it is insecure.

The mischance principle still applies to contemporary contexts. A person who chooses to post about themselves on social media has little expectation of privacy, as they at least recognize that the people who follow them are likely going to see what they posted. While the example that McArthur (2001) provided is faulty, the principle itself seems to remain sound. As for the voluntary principle, the choice to use or not to use certain services has been shrinking as our reliance on the internet has been expanding. According to Pew, 63 percent of adults believe it is impossible to go through daily life without their data being collected by the government, with the percent of adults believing the same to be true with companies being 62 percent. Further, a shockingly low 4 percent of adults say they understand a great deal about what the government is using their data for, with the percent of adults saying they understand a great deal about what companies are using their data for being slightly greater at 6 percent (Pew, 2019). Put simply, people should not have to make major sacrifices to ensure that their constitutional rights are protected.

In the *Katz* case, it was said that, by closing the door to the public telephone booth, Katz was signaling that he intended to ensure that his conversation, although held in a semi-public space, remained private. It was this signaling that the Justices used to say that a reasonable person would have expected their conversation to be private if they were in a similar situation to Katz. Like that scenario, if a person signals that they wish to ensure that their communications on the internet are private, then it should follow that a reasonable person would expect those

communications to be private. As a result, the voluntary principle ought to be framed by the understanding that a person's steps to ensure their privacy should change the standard of reasonability with which their situation has to be assessed.

Adapting McArthur's (2001) principles to the contemporary age, a person can maintain a reasonable expectation of privacy on the internet so long as: (1) the information could not be readily found by another person without a concerted effort, and (2) the person seeking to maintain their privacy did not voluntarily expose their information to the public. An example would be a person's notes that are stored in a cloud-based system. To access these notes, a government official would need to acquire a warrant.

It is important to remember that, while McArthur's (2001) principles largely concern the data collection conducted by companies rather than the government, the third-party doctrine allows the government to acquire the same information from those companies relatively easily. Therefore, any regulation that impacts how companies collect data is likely to also shape how the government is able to collect data. Additionally, the purpose for changes to privacy law is not to make it impossible for the government to acquire data on people they suspect of crimes. In fact, it is not even to make it substantially more difficult. The purpose of changes to privacy law is to ensure that constitutional rights are not infringed.

It will be useful now to return to the case of *United States v. Jones* (2012) as it concerns a drastic shift in privacy jurisprudence as it validated a mosaic theory of the Fourth Amendment. *Jones* represented a departure from the traditional understanding of the Fourth Amendment in the sense that it validated a mosaic theory. This mosaic theory states that, instead of examining potential violations of the Fourth Amendment individually, we may look at a violation as a collection of smaller offenses. Justice Sotomayor, in her concurring opinion, wrote: "[A]t the

very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'" (*United States v. Jones*, 2012, p. 955). Instead of looking at one instance, we can see how a series of instances builds a larger picture. Justice Sotomayor, citing Justice Alito, rather plainly says, "the same technological advances that have made possible non-trespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations" (*United States v. Jones*, 2012, p. 955).

Much like how McArthur (2001) proposed principles by which we can assess an expectation of privacy's reasonability, the *Jones* decision allows us to further refine our principles by allowing a review of long-term monitoring as a single entity rather than a group of individual events. It should be noted that the *Jones* decision and the coming suggestions are not seeking to completely halt police and government surveillance of the general public. Such surveillance serves a legitimate purpose in preventing various forms of cybercrime and fraud and, in some cases, aligns with the interests of public safety (Gray et al., 2013). But, by its nature, mass surveillance infringes the constitutional right to privacy of individuals. Therefore, certain restrictions are necessary to ensure that police are able to carry out their duties while also respecting constitutional limitations to their powers.

Another point worth noting is that of public exposure. The Supreme Court has long held that what a person chooses to expose to the public does not fall under a reasonable expectation of privacy. There are some who argue that GPS tracking is no different from a person engaging in their activities in public view. But what differentiates GPS tracking from simple visual surveillance is its potential duration and its persistence. Penney (2007) notes, "[w]hile we necessarily take the risk that our public behavior will be observed by others, these observations are typically sporadic and fleeting...GPS and wireless telephone tracking systems allow

authorities to surreptitiously monitor and record people's movements in a systematic and detailed manner over an indefinite period of time" (517).

Lastly, the third-party doctrine no longer appears to align with a reasonable expectation of privacy. While the information at the disposal of third parties was narrowly tailored in the days of the *Miller* and *Smith* decisions, the information that third parties access today is all-encompassing. Home security systems build a detailed record of a person's comings and goings. Cell phones track our movements, internet searches, phone calls, text messages, and emails. Fundamental to the third-party doctrine is the notion that a person has voluntarily surrendered information to that third party. But when so much information is being shared, largely without our knowledge or understanding, we can hardly call that voluntary. Brenner (2005) notes that the third-party doctrine means "[t]he focus [of police investigation] shifts from official intrusions into spaces under my temporary or permanent control to the acquisition of evidence from sources over which I exercise no control. I become irrelevant except as the object of the data acquisition" (63).

What can we say is a reasonable expectation of privacy in the digital age? First, so long as information could not be found without a concerted effort on the part of another person and the person seeking to maintain their privacy did not voluntarily expose their information to the public, it may be considered reasonable under McArthur's (2001) principles. Second, a violation of our expectation of privacy can be judged as a whole rather than a series of violations. Third, mere public exposure is not enough to suggest that a person has no reasonable expectation of privacy due to the persistence of GPS technology. Fourth, the control of information by third parties does not suggest that the information is not protected by an expectation of privacy that most people would be willing to consider reasonable.

Thus, having established what we consider to be reasonable, what needs to change?

Revisiting the Third-Party Doctrine

The third-party doctrine has become outdated. The amount of data that is held by third parties, such as Internet Service Providers and cell phone companies, has far exceeded that which was held by banks when the third-party doctrine was established. Furthermore, relying on the Supreme Court to rule on every perceived Fourth Amendment violation related to the third-party doctrine is unworkable, as the Court can only hear so many cases. To remedy this, states ought to pass legislation requiring that police obtain a warrant before they are able to access information held by third parties, such as location information, stored data, or transmitted data. Utah has already done so and should serve as an example for other states (Utah State Legislature, 2019).

It is important to remember that such a law would not make it impossible for police to continue to do their jobs. What it will do, however, is ensure that police are following constitutionally mandated guidelines regarding the right to privacy. Furthermore, with state legislatures enacting laws, as opposed to waiting on the court system to address the problem, the process is quicker and easier to adjust if problems arise in the future. Simply put, requiring police to obtain a warrant before they are given access to information held by a third party not only ensures that the Constitution is being upheld but will also make challenges to police-obtained evidence more difficult as they will be operating under the authority of a judge. In other words, both advocates for privacy rights and advocates for the police gain something with this compromise.

In the absence of such laws, police obtaining information from third parties without the consent of the owner of the information or without a warrant are essentially issuing general

warrants. The third-party doctrine needs to be revisited and revised to better reflect the scope of information that third parties now hold.

Clarification

People are not fully aware of the massive scope under which data harvesting operates. Furthermore, they are not fully aware of how their information is being stored and used. It has been said that there is an inherent assumption of risk that people take when they use certain services, which allows police to act without a warrant. However, an assumption of risk is valid if and only if the person assuming the risk is completely aware of the circumstances. If not, then the assumption of risk is done under false pretenses. While people can figure out exactly what their information is being used for and how it is being stored, the process is long and arduous, so much so that, for many people, the benefits do not outweigh the costs. People should not have to sacrifice modern conveniences and established standards in order to feel secure.

By simplifying the process of learning about what information is being collected about an individual, we again see a potential for mutual benefit. For the general public, they are able to better understand how they interact with the information environment and the assumption of risk they are taking on is validated by their knowledge. Police officers and other government officials avoid potential dismissal of evidence because any argument about vagueness or lack of access to information is no longer valid.

The European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) provide examples of how privacy regulations can enhance the rights of consumers and the general public while not being so protective as to make the jobs of police and government officials impossible or overly burdensome.

Redefine Reasonability

The GDPR provides a sturdy example of how a general United States privacy act could frame privacy as a fundamental right. Recital 2 states, “The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data.” (GDPR, 2021) Of course, in the interest of protecting the ability of the police and government officials to do their jobs, the right to privacy is qualified. Recital 4 presents a possible starting point for us, stating, “[t]he right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality” (GDPR, 2021).

The CCPA, being a law created in the United States, may be more appropriate. Important to note, the CCPA does not apply to the government or government officials. This means that, if a government agency is the one who is collecting data on an individual, a person cannot use the rights they gained under the CCPA, which include the right to know which of their data is being collected on them by companies, the right to correct false information, and the right to delete their information, among many other rights (California Legislative Information, 2021). What a nationalized version of the CCPA could do, however, is to help establish a standard for what we may consider to be a reasonable expectation of privacy, as well as curb the ability of the governmental agencies to access third-party information on individuals. Whether the GDPR or on the CCPA shapes the redefined standard of reasonability does not matter, as the two are similar. What does matter is that some redefined standard is created soon as technology will only develop more quickly over time.

Conclusion

In their landmark paper, Warren and Brandeis (1890) begin by saying, “That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.” (p. 193) Much like how Warren and Brandeis were reacting to the ability of cameras to invade the private lives of individuals, scholars today are reacting to the ability of the internet to invade the private lives of individuals. As technology advances in its sophistication and its capabilities, the public is required to rethink how they interact with that technology and how that technology may encroach on their lives. Technology shows no signs of slowing down in its developmental pace, meaning that the public will have to think more about their privacy more often than they may have been used to in the past.

Some scholars have argued that the standards with which we currently assess privacy are outdated in the face of technological advances. For example, Price (2012) argues for a three-step test which requires first determining whether the issue at play involved “papers” as defined by the Fourth Amendment, second determining whether there was a search or seizure, and third whether a warrant is required with a general assumption that a warrant will be required. Notably, Price’s approach means a search has occurred if the data found is not publicly available and a seizure has occurred when “there is some meaningful interference with an individual's possessory interests in the information, which includes the copying of data.” (Price, p. 270) Such an approach appeals to the individual liberty activists but does little to compromise with government interests. Therefore, such an approach may not be the most effective.

Langenderfer and Miyazaki (2009) choose to focus on the shift from government surveillance to private collection of data by companies. Such data collection, they argue, is a

direct threat to our ability to define ourselves. When all we are is a collection of variables, we begin to lose our individuality. So, instead of viewing privacy standards as protection from government intrusion, Langenderfer and Miyazaki frame it as a protection of who we are.

While rethinking the standards we use to assess privacy are useful, the *Katz* standard still seems useful. While it is undeniably necessary that we determine a new standard of a reasonable expectation of privacy, the *Katz* standard itself is general enough to stand the test of time. Price's test too heavily favors the public and Langenderfer and Miyazaki are too quick to discount the role that the government plays in mass surveillance. Goetz (2011) argues for a "totality of the information" approach to Fourth Amendment jurisprudence. Such an approach, also known as the mosaic approach, would examine "(1) the length of time during which the search was performed, (2) the type of information obtained, and (3) whether that information has been voluntarily conveyed to the public." (p. 852)

Mund (2017) expands on the approach by suggesting that social media activity also deserves Fourth Amendment protection. In fact, Mund believes that government monitoring of social media "invades an even greater privacy interest than that of the home." (p. 259) Mund's approach, however, is far too protective of the right to privacy. While the content of an individual's private social media page or messages deserve some form of protection, the suggestion that the contents of private social media are more important than what is done in the home lacks rigor.

Goetz's approach provides a balance between public interests and those of the government. It supports the public interest by preventing unwarranted long-term surveillance and relying on voluntary disclosure of information and it supports the government's interest by still allowing for focused surveillance on suspects. While Goetz's approach may not be the exact

approach that is adopted by every state legislature or by the federal government, it is highly likely that a similar approach will be used in the near future. Although a brief discussion was given to such standards in this thesis, a future thesis will likely explore standards such as these in further detail.

This thesis primarily focused on the implications of government surveillance and provided only a cursory overview of surveillance being conducted by companies. Surveillance conducted by companies deserves its own thesis and the ways in which the government and companies have cooperated - or, in some cases, not cooperated - warrants further discussion. A future thesis may examine how surveillance conducted by companies has increased over time and how that interacts and grows with government surveillance. Further, the current debate surrounding Section 230 of the Communications Decency Act may warrant its own discussion. That being said, starting with surveillance conducted by the government seems to be a logical first step.

This thesis is also limited in the sense that the Supreme Court is likely to hear cases regarding the issues discussed here in the future. Naturally, it is not possible to say exactly what the Supreme Court will hear in the future let alone what they will decide. But, given the growing public attention to issues surrounding technology and surveillance, it should not be a surprise to see an increase in court cases regarding privacy and technology in the near future. So, the nature of works similar to this one is that they will become outdated in a few years.

In conclusion, the concept of the right to privacy is in constant flux and is difficult to pin down. A review of Supreme Court cases regarding the right to privacy demonstrates that the Court does recognize that such a right exists even though it has not been enumerated in the Constitution. The Court has also recognized that there are a variety of circumstances in which

this right to privacy is implicated. These cases, however, do not seem to have kept up with the pace of technological development. While some cases have addressed recent technological advancements, more work is necessary. Furthermore, a unifying standard of a reasonable expectation of privacy when using the internet or similar technologies needs to be established to avoid vagueness on the issue. The third-party doctrine also needs to be returned to as it presents a variety of issues today as the amount of data collected by third parties has grown exponentially since the time of the inception of the third-party doctrine. Finally, a GDPR or CCPA type of privacy law on the federal or state level may be necessary in order to make the transition into the late digital age easier to accommodate.

References

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019, November 15). *Americans concerned, feel lack of control over personal data collected by both companies and the government*. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/

Brenner, S. W. (2005). The fourth amendment in an era of ubiquitous technology. *Mississippi Law Journal*, *75*, 1–94.

Recital 2: Respect of the fundamental rights and freedoms. (n.d.). Intersoft Consulting. https://gdpr-info.eu/recitals/no-2/

Goetz, D. H. (2011). Locating location privacy. *Berkeley Technology Law Journal*, *26*(1), 823–858.

Gray, D., Citron, D. K., & Rinehart, L. C. (2013). Fighting cybercrime after United States v. Jones. *The Journal of Criminal Law and Criminology*, *103*(3), 745–801.

Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the information economy. *The Journal of Consumer Affairs*, *43*(3), 380–388.

McArthur, R. L. (2001). Reasonable expectations of privacy. *Ethics and Information Technology*, *3*, 123–128.

Mund, B. (2017). Social media searches and the reasonable expectation of privacy. *Yale Journal of Law and Technology*, *19*(1), 238–273.

Penney, S. (2007). Reasonable expectations of privacy and novel search technologies: An economic approach. *The Journal of Criminal Law and Criminology*, *97*(2), 477–529.

Price, M. W. (2015). Rethinking privacy: Fourth amendment "papers" and the third-party doctrine. *Journal of National Security Law and Policy*, *8*, 247–299.

H.B. 57 Electronic Information or Data Privacy. (2019.). Utah State Legislature. https://le.utah.gov/~2019/bills/static/HB0057.html

Warren, S. D., & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review*, *4*(5), 193–220.

U.S. Supreme Court Cases

Bowers v. Hardwick, 478 U.S. 186 (1986)

California v. Ciraolo, 476 U.S. 207 (1986)

Carpenter v. United States, 138 U.S. 2206 (2018)

Eisenstadt v. Baird, 405 U.S. 438 (1972)

Goldman v. United States, 316 U.S. 129 (1942)

Griswold v. Connecticut, 381 U.S. 479 (1965)

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

Kyllo v. United States, 533 U.S. 27 (2001)

Lawrence v. Texas, 539 U.S. 558 (2003)

Meyer v. Nebraska, 262 U.S. 390 (1923)

NAACP v. Alabama, 357 U.S. 449 (1958)

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

Pierce v. Society of Sisters, 268 U.S. 510 (1925)

Planned Parenthood v. Casey, 505 U.S. 833 (1992)

Riley v. California, 134 U.S. 2473 (2014)

Roe v. Wade, 410 U.S. 113 (1973)

Smith v. Maryland, 442 U.S. 735 (1979)

United States v. Jones, 132 U.S. 945 (2012)

United States v. Karo, 468 U.S. 705 (1984)

United States v. Knotts, 460 U.S. 276 (1983)

United States v. Miller, 425 U.S. 435 (1976)