The Evolution of the Fourth Amendment to the United States Constitution in the Digital Age

Chris Davis

Bellevue University

CYBR-650: Current Trends in Cybersec

Winter Term, 2020

Abstract

Few rights have been so wildly affected by the rapid pace of technological change as that of the individual's right to be free from unreasonable searches and seizures provided by the Fourth Amendment to the United States Constitution. Throughout the more than two centuries since its ratification, various courts have attempted to shape and mold the Fourth Amendment's original meaning to balance the government's needs against individual's expectations of privacy in a modern day digital, connected world. Research shows that modern day knowledge of what data is being legally collected by the government and trust that such data will be stored in a way which maintains individual privacy are both quite low.

Keywords: Privacy, Constitutional Rights, Cybersecurity

The Evolution of the Fourth Amendment to the United States Constitution in the Digital Age

Introduction

Since its 1791 ratification, 220 years ago, the precise wording of the Fourth Amendment to the United States Constitution has served as a guide against which forced governmental inspection of American citizens' persons, homes, and effects have been measured.

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (U.S. Const. amend. IV, 1791).

When the Fourth Amendment was ratified, these words covered every conceivable possibility in which the government might seek to either search or seize an individual's property, but times have changed. The dawn of the Information Age brought with it a myriad of changes in how information is possessed and used. The limits of individual citizens' rights under the Fourth Amendment, as applied to digitized information, were created through the decisions of various courts over the years. This research incorporates and explains applicable court cases relevant to the Fourth Amendment from the 20th and 21st centuries, drawing interpretations from those court decisions in an analysis on how they impacted U.S. digital privacy laws today.

Origins of the Fourth Amendment

In the early days of the American Colonies, the government's ability to search or confiscate a person's belongings or home was governed by English Law. In those days,

individual privacy was not viewed as a person's *right*, but some court rulings in England did seek to apply such a right to individuals in specific roles. Take, for instance, *Semayne's Case*, an English court case dating back to 1604, in which Sir Edward Coke, then Attorney General of England made the argument,

> That the house of everyone is to him as his castle and … if thieves come to a man's house to rob him, or murder, and the owner or his servants kill any of the thieves in defence of himself and his house it is not felony, and he shall lose nothing (Semayne's Case)

Through this verdict, Sir Edward Coke created what is now known as "Castle Doctrine", the idea that a person's home is their castle and should be rigorously defended as such. In making this argument, Sir Edward Coke further specified that these provisions should not apply to the King's Men, a term used to describe officers reporting directly to the King of England. In the modern day, this can be seen as equivalent to the distinction between federal officers and state, county, and city level officers.

During this time period, it was commonplace for the courts to issue Writs of Assistance, general search warrants issued by provincial courts to assist the British government enforcement of trade and navigation laws (Britannica, 2020). Though these writs of assistance were typically carried out by customhouse officers and specified neither the house to be searched nor the goods to be searched for, they always required the assistance of the local police upon execution. These writs proved to be extremely controversial among the American Colonists, being challenged in court no less than twelve times, and continued to be a major point of contention in the time period leading up to the Revolutionary War and America's independence from British rule.

Though *Semayne's Case* established the right of a homeowner to defend their home as if it were their castle in 1603, it was not until 1763 that a case was brought before the British Court

System to challenge the government's right to trespass on privately held land and search a person's home and belongings without a written order from the courts. In the case, *Entick v. Carrington*, the plaintiff was said to have been in possession of seditious papers, leading to the Lord of Halifax issuing an order directing the four named defendants to forcibly enter Entick's property, search it, and confiscate any papers, bank bills, or any other valuable papers found therein (Teacher, 2013). At issue, in this case, was the overly broad nature of the issued order with the direction that all the defendant's papers be taken proved to be contrary to the nature of English law at the time due to the fact that such actions "would destroy all the comforts of society; papers are often the dearest property a man can have" (Teacher, 2013). The decision in *Entick v. Carrington* helped to set the groundwork for a personal expectation of privacy in Britain and its colonies, including the American Colonies.

Distant Historical Case Law Review

After America declared its independence from Britain in 1776 and ratified the Bill of Rights in 1791, no landmark cases in American judicial history set precedent using the Fourth Amendment for almost a hundred years (Search and seizure - further readings, n.d.). The first major case in American case law which involved the Fourth Amendment occurred in 1886, with the case of *Boyd v. United States*. In this case, the plaintiff, an importer, was compelled by law to produce documents demanded by the government at trial or be found guilty of the accusations against him by default. The US Supreme Court agreed to hear this case after receiving a writ of certiorari, a judicial process which requests a higher court review a lower court's decision, alleging that such a practice was an unconstitutional violation of a person's Fifth Amendment right against self-incrimination. In their opinion, the Supreme Court Justices agreed that such a

practice of requiring persons to produce inculpatory evidence against them in a forfeiture suit violated both the plaintiff's Fourth and Fifth Amendment rights (Boyd v. United States - 116 U.S. 616, 6 S. Ct. 524, 1886). This decision established the groundwork for future Fourth Amendment protections being applied to the search and seizure of a person's "papers" and would become the cornerstone upon which future decisions regarding digital data were to be based.

These protections, though created by way of the Supreme Court's ruling in *Boyd v. United States*, were subject to much discussion by the courts in the following years, leading to another major Fourth Amendment ruling in the case of *Weeks v. United States*. This case centered around the government's warrantless search by federal officers of Weeks' home and the subsequent seizure of certain papers from within, which were then presented as inculpatory evidence at trial against him. In their judgement, the US Supreme Court Justices unanimously held that the warrantless search of Week's home was a direct violation of Weeks' Fourth Amendment rights and that the government's refusal to return Weeks' documents also violated his Fourth Amendment rights (Weeks v. United States, 1914). This decision is particularly noteworthy in that the US Supreme Court not only held that the evidence in this case was obtained in violation of Weeks' Fourth Amendment rights, but also that any evidence collected by a federal officer which was in violation of a person's Fourth Amendment right must be excluded from being used as evidence against that person at trial. This was the first application of what would come to be known as the "exclusionary rule" in modern day law.

As with the prior decision in *Boyd v. United States*, so too had the decision in *Weeks v. United States* became the topic of much judicial debate, owing mainly to the specific wording of the Supreme Court's ruling, which stated in part,

> Where letters and papers of the accused were taken from his premises by an official of the United States, acting under color of office but without any search warrant and in violation of the constitutional rights of accused under the Fourth Amendment, and a seasonable application for return of the letters and papers has been refused and they are used in evidence over his objection, prejudicial error is committed, and the judgment should be reversed. (Weeks v. United States., 1914)

In this context, the specific meaning of the phrase "official of the United States" was understood to encompass only federal agents, thus excluding any state level law enforcement officers from being held to the Supreme Court's decision in *Weeks v. United States*.

This issue was brought back to the Supreme Court in 1961 with the case of *Mapp v. Ohio*. In this case, the plaintiff's home was forcibly entered by police officers without a warrant after she had previously denied them entry without such a warrant. Mapp's home was then searched for "obscene materials", which were found by officers in a steamer trunk located in the building's basement. This case presented numerous issues prima facie, with the most notable being that the Ohio State Supreme Court specifically called out the unconstitutionality of the entry and subsequent search of Mapp's home yet still chose to allow the evidence collected as a result of that search be used against Mapp at trial.

The US Supreme Court disagreed with the notion that their previous decision in *Weeks v. United States* did not apply to state courts, stating specifically, "All evidence obtained by searches and seizures in violation of the Federal Constitution is inadmissible in a criminal trial in a state court" (Mapp v. Ohio, 1961). With this decision, the US Supreme Court affirmed that the rights afforded an individual by way of the Fourth Amendment apply equally in all American

criminal courts, and, in so doing, solidified the meaning of what is now known as the "exclusionary rule" in modern law to be applicable to both state and federal cases alike.

Up to this point in American legal doctrine, the courts had not made any firm decisions as to how the Fourth Amendment's protections applied to the rapidly emerging wealth of technology available to ordinary citizens. The first US Supreme Court case involving technology from the dawn of the Digital Age was the case of *Katz v. United States* in 1967. In this case, Katz was suspected of transmitting gambling information to clients in other states through his use of public telephone booths. This led federal agents to attach an electronic eavesdropping device on the outside of a public phone booth Kats was known to frequent.

Through the use of this device, agents were able to obtain recordings of Katz's conversations from said phone booth, which were presented against him at trial and used to convict Katz of eight counts of 'illegal transmission of wagering information' at trial. On appeal to the US Court of Appeals, the crux of the prosecution's argument for the introduction into evidence of the recordings obtained via the use of this electronic eavesdropping device was that no physical intrusion was made in order to gather the recordings. This argument was based solely upon the fact that the eavesdropping device was placed outside the public phone booth used by Katz.

In a 7–1 decision, the US Supreme Court disagreed with the supposition that any physical intrusion was required to bring Fourth Amendment protections into consideration. There are two main conclusions drawn from Justice Stewart's opinion in *Katz v. United States*. The first is that the Fourth Amendment protects people, not places. It was this logic which led the Supreme court to conclude that Katz's right to privacy had been violated despite the lack of physical intrusion by the government in recording Katz's communications. The second is that information which a

person knowingly exposes to the public is not covered by the Fourth Amendment's privacy protections. This logic gave rise to what is now known as the "Third Party Doctrine" in modern law, which generally stipulates that information provided to a third party is not protected against warrantless search and seizure by the government.

Justice Harlan, in writing a concurring opinion for this case, introduced the idea of a person's individual expectation of privacy through the creation of a two-part 'reasonableness' test, which has now come to be known as the 'Katz test' in modern law, writing:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable." (Katz v. United States, 1967)

The ruling in *Katz v. United States* is particularly remarkable not only because of the long-lasting impact of Justice Harlan's 'Katz test', but also because the US Supreme Court specifically cited that information openly shared in public is not subject to Fourth Amendment protections. In so doing, the 'Katz test' also created the "plain view doctrine", which states that anything in plain view can be viewed without a warrant. This specific ruling and interpretation of the Fourth Amendment's protections, though seemingly intuitive, was the first time such a

determination was made and helped to form yet another bright line as to what information could be reasonably expected to be considered private by a person.

The next landmark Fourth Amendment decision from the US Supreme Court came in 1979, with the case of *Smith v. Maryland*. In this case, a woman named Patricia McDonough was robbed in Baltimore, Maryland. After the robbery occurred, McDonough gave police a good description of her attacker and the vehicle her attacker was driving. In the following days, she began receiving threatening phone calls, with one instructing her to stand on her porch where she watched as her attacker's vehicle drove past her home. Police were correlated the car's license plate number to a man named Michael Lee Smith. Without a warrant, police then used this information to request that a pen register, a device which only records digits dialed by a customer, be placed on Smith's phone line by the telephone company. Police then used the pen register data to determine Smith was the source of these threatening calls. This led police to obtain a search warrant for his residence where they found a public phone book with the page containing McDonough's number having its corner turned down. Smith was later placed in a lineup and positively identified by McDonough, leading to his arrest and subsequent conviction.

The US Supreme Court's decision in this case made clear that "Fourth Amendment protections are only relevant if the individual believes that the government has infringed on the individual's reasonable expectation of privacy" (Smith v. Maryland, 1978). Because a pen register only recorded the part of a call which was sent to the telephone company specifically to service and route the call, the panel opined, this information was therefore considered to be 'public', and was not subject to the protections of the Fourth Amendment. The US Supreme Court decision in this case was significant, as it further clarified the line defined in *Katz v. United States* separating 'public' information, to which no Fourth Amendment protections apply,

from ‘private’ information, which should fall under the realm of protection under the Fourth Amendment.

Starting with their decisions in *Boyd v. United States* and *Weeks v. United States*, the US Supreme Court began to define how individuals’ homes and belongings could be searched and seized by the government while maintaining a balance between individual freedoms and governmental interests by introducing the “exclusionary rule”. The US Supreme Court further extended the “exclusionary rule” to be applicable to evidence obtained in State Courts as well in *Mapp v. Ohio*. With their decision in *Katz v. United States*, the US Supreme court established a reasonableness test, commonly known as the “Katz test”, and the “Third Party Doctrine”, both of which served to clarify the difference between ‘public’ information and ‘private’ information. With the decision in *Smith v. Maryland*, the US Supreme Court further expanded the scope of information which falls under the “Third Party Doctrine”. These decisions help to form the basis upon which more modern court cases base their logic when applying the Fourth Amendment’s interpretations to the complex maze of digital data in the late 20th century.

Recent Historical Case Review

In more recent US Supreme Court decisions, *United States v. Jones* is one of the first to specifically address the issue of privacy with a focus on digital surveillance methods. In this case, Jones was suspected of trafficking in narcotics, leading federal officers to secure a warrant to track the whereabouts of his wife’s vehicle via the use of a Global Positioning System (GPS) transponder. That warrant specified that the GPS transponder was to be attached within ten days, to the vehicle when it was physically located in the District of Columbia. The GPS transponder was not actually attached until the eleventh day, when the vehicle was physically located in the

state of Maryland. It was then left to collect data for the next twenty-eight days. The District of Columbia District Court ordered that any data obtained while the vehicle was parked at Jones' home was inadmissible. The remainder of the data was allowed be used as evidence against Jones as its collection occurred while Jones was traversing public roadways, to which no inherent expectation of privacy existed. This case was won by the defendant on appeal with the District of Columbia District Court, but the US government chose to appeal the decision to the US Supreme Court, which upheld the District Court's ruling in the case. In the majority opinion, Justice Scalia was very clear about why the US Supreme Court decided as it did, stating,

> It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted. (United States v. Jones, 2011)

With the judgement in *United States v. Jones*, the US Supreme Court once again redefined the guidelines which lay out American citizens' protections against unreasonable searches as defined by the Fourth Amendment in the Digital Age. Justice Scalia made this point quite clear in the majority opinion statement saying, "we must assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted" (United States v. Jones, 2011). The statement exemplifies the understanding that technology has given rise to entirely novel methods with which to obtain information which is not necessarily public knowledge from citizens and that the Fourth Amendment's protections must evolve as well.

In a concurring opinion, Associate Justice Sotomayor also wrote about Fourth Amendment protections in the Digital age saying,

> More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. (United States v. Jones, 2011)

This statement is quite important, as it shows understanding that the intent behind the Fourth Amendment should apply equally to modern day technology as it did to the technologies which were available at the time of its inception. It also serves to undermine the bright line established with the opinion in *Katz v. United States*, implying that even information which is voluntarily disclosed to third parties may still have some reasonable expectation of being kept private.

Two years after *United States v. Jones* came another landmark decision from the US Supreme Court, in the 2013 case of *Riley v. California*. In this case, Riley was pulled over as the vehicle he was driving displayed expired registration tags. Due to Riley's license being suspended at the time, his car was required to be impounded. As part of the impound process, an inventory search is usually undertaken of the vehicle, which, in this case, resulted in the discovery of two firearms, leading to Riley's arrest. A cursory pat down for weapons and contraband is typical after arrest, which showed Riley to have a cellular telephone on his person. The arresting officers seized this device, and a subsequent search found many terms they thought to be gang related. The phone was turned over to officers from the Gang Unit, who then further analyzed its contents, without a warrant of any kind, and used that information to link Riley to the Lincoln Park Gang of San Diego, California. This information was presented against Riley at trial and used to convict him. Riley appealed his case on the grounds that the search of his phone pursuant to his arrest was a violation to his Fourth Amendment right to unreasonable searches.

The US Supreme Court agreed unanimously with Riley's claims and overturned the lower court's ruling on the grounds that the search of Riley's phone was indeed a violation of Riley's Fourth Amendment rights. Justice Roberts wrote the point quite clearly in the court's opinion saying, "The police generally may not, without a warrant, search digital information on a cell phone seized from an individual who has been arrested" (Riley v. California, 2013). The Court supports this point by clearly stating,

> Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Officers may examine the phone's physical aspects to ensure that it will not be used as a weapon, but the data on the phone can endanger no one. (Riley v. California, 2013)

It is important to note that the decision in *Riley v. California* does not make the search of a cell phone incident to arrest in and of itself unconstitutional, but rather it requires that a warrant be obtained before such a search in accordance with the Fourth Amendment's protections against unreasonable search and seizure. This marks the first US Supreme Court decision in which the court tackles the topic of what is reasonable, in relation to searching digital devices like cellular telephones, and lays out specific guidelines on when such searches are permissible without the presence of a warrant.

In the same year as *Riley v. California*, the US Court of Appeals for the Ninth Circuit issued a major decision affecting the Fourth Amendment and its applicability to warrantless searches of technological devices at international border crossings in the case of *United States v. Cotterman*. In this case, Cotterman was returning home to America from travelling abroad in Mexico when he was stopped and selected for secondary screening at the border crossing in Lukeville, Arizona based upon an alert for his presence in a governmental database due to his

frequent travels, previous conviction for child molestation, and his crossing from Mexico, a country "well known for sex tourism" according to the Department of Homeland Security (United States v. Cotterman - 709 F.3d 952 (9th Cir.), 2013).

As part of this screening, Cotterman was required to submit to searches of his digital devices. The initial search at the border crossing turned up no data to indicate the presence of any contraband materials on his devices, but his laptop was seized and sent to an off-site digital forensics laboratory for further forensic analysis. During this forensic analysis, evidence of child pornography was found on Cotterman's laptop which was subsequently used against him at trial and led to his conviction. This evidence was originally ruled as inadmissible by the US District Court which heard the case, but this decision was overturned by the US Court of Appeals for the Ninth Circuit on appeal from the US government.

In the Court's opinion on this case, Judge McKeown specifically calls out the need for a balance to be struck between the government's need to secure its borders and an individual's right to privacy saying,

> Although courts have long recognized that border searches constitute a 'historically recognized exception to the Fourth Amendment's general principle that a warrant be obtained,' … reasonableness remains the touchstone for a warrantless search. Even at the border, we have rejected an 'anything goes' approach [to warrantless searches]. (United States v. Cotterman - 709 F.3d 952 (9th Cir.), 2013)

The Court further expands on the gravity of this case in regard to Fourth Amendment rights in the Digital Age in their opinion saying,

> This watershed case implicates both the scope of the narrow border search exception to the Fourth Amendment's warrant requirement and privacy rights in commonly used

> electronic devices. The question we confront 'is what limits there are upon this power of technology to shrink the realm of guaranteed privacy' (United States v. Cotterman - 709 F.3d 952 (9th Cir), 2013).

The US Court of Appeals for the Ninth Circuit's decision in *United States v. Cotterman* addresses the topic of what constitutes an invasive search of a digital device, and what limits should be placed upon such an intrusion to devices and realms which contain so much private and sensitive information. The Court's opinion in this case is quite clear that digital devices such as laptops, cell phones, tablets, and digital cameras contain significant amounts of data which would fall under the protections of the Fourth Amendment from unreasonable search by the government. The Court also notes their ubiquity in modern day life for the millions of travelers crossing into and out of the United States' borders every day. The US Supreme Court opinion in *Riley v. California* supports this same ideology, observing that digital devices collect "in one place many distinct types of information that reveal much more in combination than any isolated record" and noting that "many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives" (Riley v. California, 2013).

Another decision from the US Supreme Court in 2017 concerning privacy rights of data sent to third parties was handed down for the case of *Carpenter v. United States*. In this case, Carpenter was suspected of being connected to a series of armed robberies after the Federal Bureau of Investigation (FBI) requested an order from a magistrate judge to obtain 'transactional records' for his phone number from the cellular network provider. This information included not only the date and time of calls placed, but also their duration and the approximate location where each call began and ended, also known as Cell Site Location Information (CSLI). The CSLI

evidence collected as a result of the order for ‘transactional records’, which was not a ‘warrant’, as recognized by the Fourth Amendment, was subsequently used at trial against Carpenter, resulting in his conviction. Carpenter argued on appeal that the warrantless collection of this data was an unconstitutional violation of his Fourth Amendment rights. The US Supreme Court agreed with Carpenter, stating that the government’s acquisition of Carpenter’s CSLI records was indeed a ‘search’ in the eyes of the Fourth Amendment. Chief Justice Roberts notes in the Court’s opinion, “The digital data at issue—personal location information maintained by a third party—does not fit neatly under existing precedents” and compares the CLSI information obtained by the FBI to that of the federal officers in *United States v. Jones* saying, “Tracking a person’s past movements through CSLI partakes of many of the qualities of GPS monitoring considered in Jones—it is detailed, encyclopedic, and effortlessly compiled” (Carpenter v. United States, 2017).

The US Supreme Court’s opinion in the case of *Carpenter v. United States* serves to strengthen their previous decisions in *Riley v. California* and *United States v. Jones* through expanding the protections afforded to location data obtained by the government without the use of a warrant. This is accomplished by noting that such CSLI data is not ‘shared’ as the term is normally used and that “cell phones and the services they provide are ‘such a pervasive and insistent part of daily life’ that carrying one is indispensable to participation in modern society” (Carpenter v. United States, 2017). Though this case did specifically enumerate the necessity of a warrant for the acquisition of CSLI, the Court did not comment on what is more broadly known as the “Third Party Doctrine”, a legal doctrine first established after the Court’s decision in *Katz v. United States* which holds that information voluntarily shared with third parties such as banks, internet service providers, telephone companies, and many other categories of service providers

have no ‘reasonable expectation of privacy’ applicable to them, meaning they can be obtained by the government and used as evidence in a trial without the requirement for first obtaining a warrant (Reitman, 2020).

The next most recent decision affecting Fourth Amendment rights in the Digital Age comes from the United States Court of Appeals for the Eleventh Circuit for the case of *United States v. Vergara*. In this case, Vergara was transiting US Customs in Tampa, Florida after returning from a trip to Cozumel, Mexico, where he was randomly selected for secondary screening. During the search of Vergara’s baggage, he was found to be in possession of multiple cell phones, which he was asked to turn on so that the Customs officer could inspect the device. This search turned up a video containing two topless female minors on one of the phones, leading the Customs officer to seize the phones and contact a Department of Homeland Security (DHS) investigator to further examine Vergara’s cell phones. This forensic examination revealed numerous pictures and videos which involved the use of a minor engaging in sexually explicit conduct. The evidence uncovered during this forensic examination was used against Vergara at trial, leading to his conviction. Vergara appealed the introduction of the evidence obtained from the forensic examination of his phones at trial, stating that without a warrant such a search violated his Fourth Amendment rights in accordance with the United States Supreme Court’s decision in *Riley v. California*.

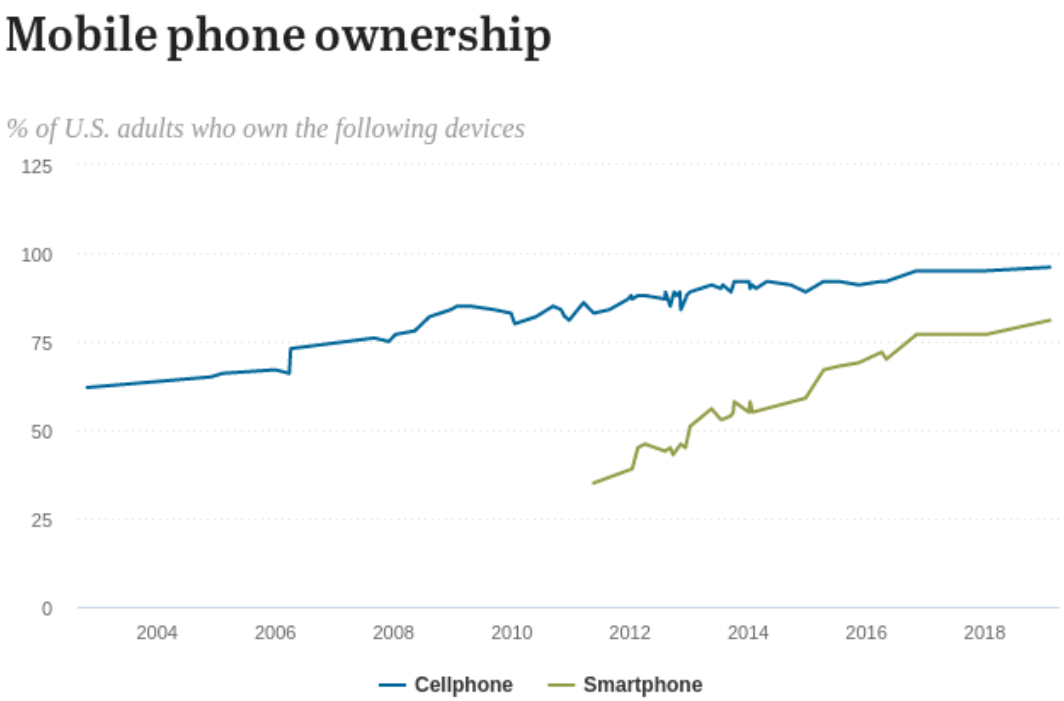
The US Court of Appeals for the Eleventh Circuit disagreed, citing the government’s interests in protecting its borders overrode Vergara’s right to privacy during a border crossing by likening the storage of imagery on his cell phones to the storing of physical pictures in a notebook, as such a notebook would’ve been subject to inspection for contraband. In this decision, the Court specifically called out the historically understood lack of a requirement for

probable cause or the acquisition of a warrant as a prerequisite to searches occurring when transiting the United States' international borders and specifically enumerated the fact that only 'reasonable suspicion' needs to exist to support such a search. 'Reasonable suspicion' is a much lower bar than the 'probable cause' the United States Supreme Court required in its *Riley v. California* decision speaking specifically about warrantless searches of cellular devices after an arrest is made.

Current Issues

Each of these rulings helped to shape how the protections of the Fourth Amendment are applied to limit governmental interloping in the personal and confidential affairs and effects of the American citizenry in a world much different than the one in which they were conceived and ratified. In the US Supreme Court's 2013 response to *Riley v. California*, the court specifically enumerates the ubiquity of cell phones in daily life and the substantial amount of data such devices can contain saying, "many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives" (Riley v. California, n. d.). Indeed, research supports this conclusion, with a Pew Research Center survey (Figure 1) showing that 96% of Americans now own a cellphone of some kind. 81% of those surveyed own a smartphone, which is up from just 35% in the Pew Research Center's first such survey in 2011.

Figure 1



With cell phones, computers, and various other methods of collecting and processing digital data so deeply embedded in most Americans' lives, the collection of their data by corporations and the government has come to be accepted as the status quo. This collection can sometimes be collected directly by governmental entities without need for a warrant, leading to the disclosure of information unintentionally. Nowhere is this point clearer than in the 2103 case of *United States v. Moalin*.

In this case, Moalin and three other men, all of Somalian descent, were suspected of financing a terrorist group in Somalia. In investigating the four men's involvement with this terrorist organization, the US government was found to have unconstitutionally retrieved data about their online activities through a National Security Agency (NSA) program known as PRISM (United States v. Moalin, 2015). This program was first revealed to the American public by the whistleblower Edward Snowden in 2013. Snowden described it then as a 'direct access'

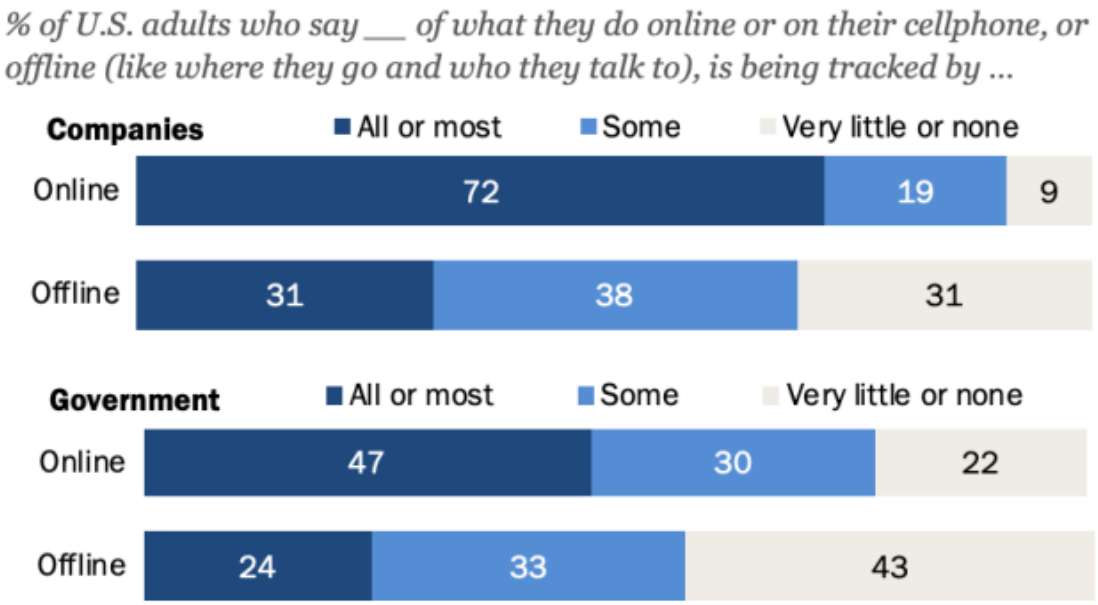
program operated by the NSA which included major internet companies like Google, Facebook, Apple, Yahoo, and Microsoft. Through this program, the NSA was able to obtain virtually unlimited amounts of metadata, or data which describes other data, about each service's users such as user ids, phone numbers, email addresses, IP addresses, electronic communications, video chats, and much more (Mezzofiore, 2014).

The Court's 2020 decision in this case is particularly unique, as it is the only case as of yet on record to specifically reference the NSA's PRISM program stating, "the panel held that the government may have violated the Fourth Amendment when it collected the telephony metadata of millions of Americans" (United States v. Moalin, 2015). The court also specifically states how different this case is from the cases which predate it like *Carpenter v. United States* and *Smith v. Maryland*, saying "Advances in technology since 1979 have enabled the government to collect and analyze information about its citizens on an unprecedented scale" and "a 'central aim' of the Fourth Amendment was 'to place obstacles in the way of a too permeating police surveillance.' " (United States v. Moalin, 2015).

This decision highlights the fact that many Americans do not really understand just how much data they are giving away in their daily lives, nor do they know who is receiving and cataloging such data. Survey data from the Pew Research Center supports this conclusion, with Figure 2 showing that a 72% majority of Americans believe their online activity is being tracked by large corporations and 47% or roughly half believe their online activity is being tracked by the government en masse.

Figure 2

Public Opinion on Tracking



Note: Respondents were randomly assigned to answer questions about how much of what they do online and on their cellphone, and offline (like where they go and who they talk to) is being tracked by "companies" or "the government." Those who did not give an answer are not shown.
Source: Survey conducted June 3-17, 2019.
"Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information"

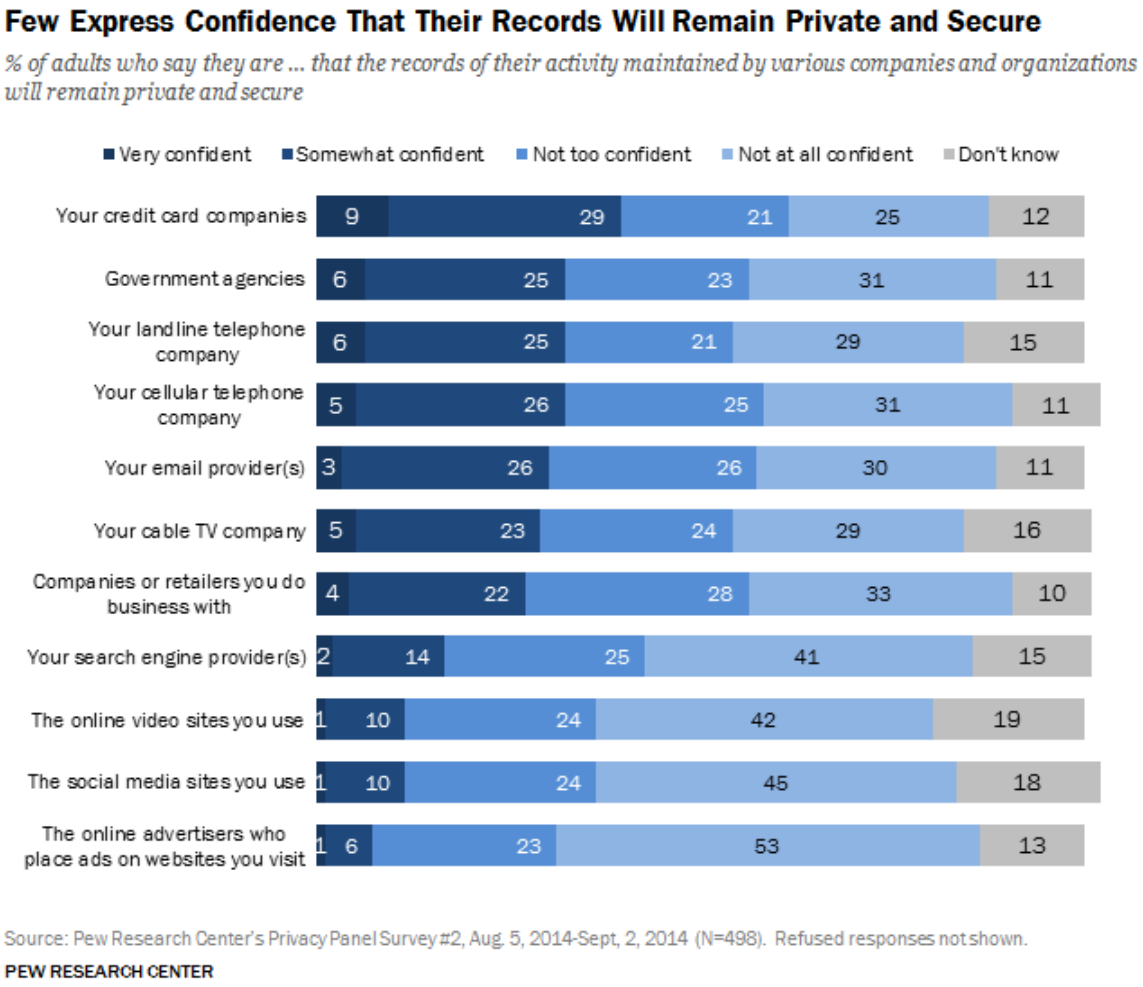
PEW RESEARCH CENTER

While other countries have passed great data protection legislation, like the European Union's (EU) General Data Protection Regulation (GDPR) and Brazil's General Personal Data Protection Law (GPDPL), America's efforts at creating the legal idea of data privacy have resulted in a tangled web of laws which stretch back over fifty years. Starting with the Federal Wiretap Act of 1968 (FWA), America has enacted numerous laws which each change the legality of digital searches including the Electronic Communications Privacy Act of 1986 (ECPA), the Stored Wire Electronic Communications Act of 1986 (SWECA), and the USA PATRIOT Act.

These are only a subset of the laws which govern governmental intrusion upon a person's Fourth Amendment right to privacy. Other data protection legislation exists which govern access to personal data held by various institutions such as the Health Insurance Portability and

Accountability Act of 1996 (HIPPA) and the California Consumer Privacy Act (CCPA). With such a dizzying array of definitions on how data should be protected and from whom, it's understandable then that Americans' opinions on how secure they expect that their data is with various entities reflects this confusion. Figure 3, a 2014 Pew Research Center survey on the topic, shows that 31% of Americans trust the government about as much as they trust the local telephone company to keep their data private and secure.

Figure 3



Conclusion

Throughout the more than two centuries since its inception, the wording of the Fourth Amendment has remained unchanged, despite the rapidly changing world in which its original intent must now be molded to fit its application to privacy in today's modern world. Judicial opinions in *Katz v. United States* and *Smith v. Maryland* have established bright line rules regarding how the right to privacy belongs to a person, not a place and how such a right should be interpreted to determine its 'reasonableness' according to the venerable "Katz test". Judicial opinions in *United States v. Jones*, *Riley v. California*, and *Carpenter v. United States* have helped to craft a framework against which each new application of governmental infringement on new technologies can be weighed to determine if such action is indeed a violation of a person's Fourth Amendment right to protection against unreasonable search and seizure. Judicial opinions in *United States v. Cotterman* and *United States v. Vergara* have established the government's power to protect its borders from the traversal of contraband with very low bars to overcome in order to perform extensive searches of a person's technological devices.

To be certain, the Digital Age has entirely changed the realms within which a person should reasonably expect to maintain their privacy, but it has also brought with it questions about when and how such 'public' data should be collected and how it should be used. Judicial opinion in *United States v. Moalin* specifically calls out the blatant disregard shown by the NSA towards American citizens' rights regarding the NSA's collection of messages, emails, calls, and locations data en masse. With such large swaths of data and metadata being collected, indexed, and cataloged by corporations and, in turn, the government, every day the water becomes ever murkier and the lines between what information is and what information is not acceptable for the government to collect about its citizens without a warrant become less and less clear.

References

U.S. Const. amend. IV (1791)

Semayne's Case. (1603). Retrieved February 06, 2021, from https://groups.csail.mit.edu/mac/classes/6.805/admin/admin-fall-2005/weeks/semayne.html

Teacher, Law. (November 2013). Entick v Carrington [1765]. Retrieved from https://www.lawteacher.net/cases/entick-v-carrington-1765.php?vref=1

Britannica, T. Editors of Encyclopaedia (2020, February 28). Writ of assistance. Encyclopedia Britannica. https://www.britannica.com/topic/writ-of-assistance

Search and seizure - further readings. (n.d.). Retrieved February 07, 2021, from https://law.jrank.org/pages/12471/Search-Seizure.html

Boyd v. United states - 116 U.S. 616, 6 S. Ct. 524 (1886). Retrieved February 07, 2021, from https://www.lexisnexis.com/community/casebrief/p/casebrief-boyd-v-united-states

Weeks v. United States. (1914). *Oyez*. Retrieved February 07, 2021, from https://www.oyez.org/cases/1900-1940/232us383

Mapp v. Ohio. (1961). *Oyez*. Retrieved February 07, 2021, from https://www.oyez.org/cases/1960/236

Katz v. United States. (1967). *Oyez*. Retrieved February 07, 2021, from https://www.oyez.org/cases/1967/35

United States v. Jones. (2011). *Oyez*. Retrieved February 8, 2021, from https://www.oyez.org/cases/2011/10-1259

Riley v. California. (2013). *Oyez*. Retrieved February 8, 2021, from https://www.oyez.org/cases/2013/13-132

United States v. Cotterman - 709 F.3d 952 (9th Cir. 2013). (2013). *LexisNexis*. Retrieved February 8, 2021, from https://www.lexisnexis.com/community/casebrief/p/casebrief-united-states-v-cotterman

United States v. Moalin. (2015, November 5). *Brennan Center For Justice*. Retrieved January 18, 2021, from https://www.brennancenter.org/our-work/court-cases/united-states-v-moalin

Carpenter v. United States. (2017). *Oyez*. Retrieved February 8, 2021, from https://www.oyez.org/cases/2017/16-402

Reitman, R. (2020, December 07). Podcast episode: Fixing a Digital loophole in the Fourth Amendment. Retrieved February 08, 2021, from https://www.eff.org/deeplinks/2020/11/podcast-episode-fixing-digital-loophole-fourth-amendment

United States v. Vergara, No. 16-15059 (11th Cir. 2018). (2018). *Justia Law*. Retrieved January 19, 2021, from https://law.justia.com/cases/federal/appellate-courts/ca11/16-15059/16-15059-2018-03-15.html

Demographics of mobile device ownership and adoption in the United States. (2020, June 05). Retrieved February 10, 2021, from https://www.pewresearch.org/internet/fact-sheet/mobile/

Mezzofiore, G. (2014, July 01). NSA whistleblower Edward Snowden: Washington Snoopers are criminals. Retrieved February 10, 2021, from https://www.ibtimes.co.uk/nsa-whistleblower-edward-snowden-479709

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, May 26). 2. Americans concerned, feel lack of control over personal data collected by both

companies and the government. Retrieved February 10, 2021, from https://www.pewresearch.org/internet/2019/11/15/americans-concerned-feel-lack-of-control-over-personal-data-collected-by-both-companies-and-the-government/