A Few Concerns of Technology's Impact on the Fourth Amendment Reasonable Expectation of Privacy

By

Ritz Carr

Submitted in partial completion for CRJS 497

Department of Sociology and Criminal Justice

Old Dominion University

Fall Semester 2023

ABSTRACT

Modern technologies have made life much more convenient to perform day-to-day tasks but have come with many Fourth Amendment protection questions regarding our Reasonable Expectation of Privacy (REP). The Fourth Amendment, among other things, protects us from unreasonable searches and seizures of the government. The issue is the breakneck speed of technology's evolution, the pace of legislation, and the Supreme Court's decisions regarding REP concerns. This paper first details important definitions- including legal definitions -needed to understand this topic, followed by a literature review and discussion. The focus of this paper will be a discussion applying important literature as well as the limitations and future research. It appears that the United States has a long way to go for developing solid Fourth Amendment REP protections adequately addressing emerging technologies.

KEY WORDS: Bring Your Own Device, Constitution, Cybersecurity, Fourth Amendment, Privacy, Reasonable Expectation of Privacy, Searches and Seizures, Smart Home Devices, Supreme Court, Third Party Doctrine

INTRODUCTION

Justice Frank Murphy wrote, “Science has brought forth more effective devices for the invasion of a person’s privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment.” (Donohue, 2021). The Fourth Amendment’s insights and applications in our modern world have surpassed anything imaginable when the Framers wrote the Constitution and the Bill of Rights. It was first understood to protect people and their property, but now, there is a whole new medium in which the Fourth Amendment can be applied to: the digital world. We have discovered that it is not as analogous to the physical world in practice as opposed to on paper, evidenced by federal laws and statues written 40-50 years ago, like the Electronic Communications Privacy Act (ECPA) of 1986. Moreover, the issue stems from our inability to predict and keep pace with technology’s explosive advancements since then.

One right people expect to have is the right to privacy, an implied Constitutional right (*Katz v. United States*, 389 U.S. 347 [1967].). More than ever is this a concern, especially in our personal ‘effects’- our devices. But, not only our devices, our homes- that, in turn, may be subject to privacy violations enabled by technology (Manning, 2019), as demonstrated by *Kyllo v. United States:* The use of a thermal imaging device from a public vantage point was used by police to detect the heat radiating off certain parts of the house to establish probable cause that Kyllo was growing marijuana in his garage (*Kyllo v. United States,* 533 U.S. 27 [2001]).

In *Katz v. United States,* Justice Harlan defined a Reasonable Expectation of Privacy (REP) through a two-pronged test, officially setting the stage for future cases regarding our right to privacy. Though situations and scenarios regarding technology and its impact on the Fourth Amendment's REP are broadening, only a handful have been addressed by the Supreme Court. What, then, are the impact and implications of emerging technology on our Fourth Amendment REP?

PURPOSE

The purpose of this paper is to provide a foundational understanding of the Fourth Amendment and its components including REP, the implications of technology in REP applications, and a few situations that involve questionable applications of the Fourth Amendment REP and advancing technologies.

SCOPE

The scope of this paper primarily addresses 21st century issues regarding technology and our REP while relying in past upon previous mid-20th century case law.

The range in disciplines covered in this paper requires an explanation of the workings of technologies and jurisprudence of the Fourth Amendment in different arenas such as: privacy and Smart Home Devices (SHDs) and the business industry and the REP in cellular searches of public and government employees.

INTENDED AUDIENCE

The intended audience for this paper is those who have some background knowledge in basic legal and cybersecurity concepts; however, the purpose of the definitions section is to provide adequate background knowledge to better understand the literature review and discussion sections of the paper. In all, all those interested in privacy, technology, constitutional law, and Fourth Amendment implications are the target audience.

DEFINITIONS

FOURTH AMENDMENT

The Fourth Amendment of the United States (US) Constitution states:

"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."(Library of Congress, US Constitution - Fourth Amendment, N.d.)

The Fourth Amendment recognizes a fundamental personal right: we cannot be searched nor can our property be seized without good reason, typically in the form of a warrant given by an established legal authority such as a non-government affiliated judge or magistrate. However, there are exceptions to the Fourth Amendment warrant requirement that will be covered shortly (Del Carmen and Hemmens, Chapter 7, 2015).

PROBABLE CAUSE

The Fourth Amendment of the Constitution provides in past:

"..and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation.." (Library of Congress, US Constitution - Fourth Amendment, N.d.).

Probable cause was defined by the Supreme Court (SCOTUS) in the case of *Brinegar v. United States*:

> *"..the facts and circumstances within the officers' knowledge and of which they had reasonably trustworthy information are sufficient in themselves to warrant a man of reasonable caution in the belief that an offense has been or is being committed."* (*Brinegar v. United States*, 338 U.S. 160 [1949]).

A "man of reasonable caution" refers to your average day-to-day citizen in this definition. If this person were to witness or be explained the situation and rationally believe that a crime was or has been committed, probable cause would be warranted (Del Carmen and Hemmens, Chapter 3, 2015).

Probable cause is the legal justification for a search and is used for both search and arrest warrants or for warrantless searches and seizures under the Fourth Amendment.

REASONABLE EXPECTATION OF PRIVACY (REP)

A landmark case for the Fourth Amendment, *Katz v. United States* helped bring a Reasonable Expectation of Privacy (REP) to light. Justice Harlan, who provided a concurring opinion to the case, defined this two-prong test:

> *"(1) the person must have exhibited an actual expectation of privacy, and (2) the expectation must be one that society is prepared to recognize as reasonable.*" (*Katz v. United States*, 389 U.S. 347 [1967]).

The REP standard has been applied to real world situations. Take the case of *Katz.* Katz was suspected of transmitting gambling information to people he knew outside his state using a public pay phone to conduct his calls. The pay phone was one he regularly used and was wiretapped by authorities. Justice Stewart wrote that Katz *did* have a reasonable expectation of privacy regarding his conversation. The government intrusion may have not been a physical one regarding visual privacy, but rather was an intrusion on Katz's audible privacy, which he did have a REP upon shutting the door to the booth (*Katz v. United States,* 389 U.S. 347 [1967]).

RIGHT TO PRIVACY

Fourth Amendment protections are extended to our personal privacy rights, as a result of the SCOTS decision in *Katz*. Seen as a 'penumbra right' or 'shadow right', the right to privacy is not explicitly defined in the Constitution but is often derived from the Fourth Amendment (Del Carmen and Hemmens, Chapter 7, 2015). Often paired together, SCOTUS cases *Riley v. California* (2014) and *Carpenter v. United States* (2018) both represent more recent guidance on our right to privacy of our devices, specifically phones and personal computers. The former held that any search incident to arrest regarding a device is not a valid search under the Fourth Amendment, as "police do not need to look at the contents of the phone to determine whether the phone is a threat to their safety." (EPIC) (*Riley v. California,* 573 U.S. 373 [2014]).

The *Carpenter* opinion, however, tackles a more difficult situation. In *Carpenter*, government authorities, without a warrant, obtained "weeks-long records", Cell-Site Location Information (CSLI) of Carpenter's movement from his cell phone carrier company. While the Third Party Doctrine (TPD), which states no one has an REP when giving data to a third party,

would be applicable in the sense of lacking an REP of information our carrier holds, it is *not* applicable to this situation of "weeks-long records" as noted:

> "*A majority of the Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which "hold for many Americans the 'privacies of life,'* " As seen in *Riley v. California,* "*contravenes (violates) that expectation.. 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,* 585 U.S. ___, 138 S. Ct. 2206 [2018])

Using those two cases as examples, this is the modern standing on our right to privacy of our devices, from smart watches to personal computers to phones. In essence, it is "the right to be let alone by other people." (*Katz v. United States*, 389 U.S. 347 [1967]).

SEARCH

The often used phrase "search and seizure" refers to two *separate* acts, not one. Defined by Ronaldo del Carmen and Craig Hemmens in *Criminal Procedure: Law and Practice*, a search is "the exploration or examination of an individual's house, premises, or person to discover things that may be used by the government for evidence in a **criminal prosecution**." (Del Carmen and Hemmens, Chapter 7, 2015).

Expanded upon in *Katz v. United States*, a search is not limited to "homes, offices, buildings, or other enclosed places; rather, it can occur in any place where a person has a

reasonable expectation of privacy, even if the place is in a public area..” (Del Carmen and Hemmens, Chapter 7, 2015) (*Katz v. United States*, 389 U.S. 347 [1967]).

Other types of searches involving technology include electronic surveillance and wiretaps which are directed to intercept the content of communications. These two, under strict guidelines, typically require a search warrant (LII – Fourth Amendment, N.d.).

SEIZURE

A seizure occurs when the government exercises control over a physical object or person for the purposes of detaining or confiscating to be further examined or investigated; typically these are items or persons that have or have been used to violate the law. A device may be subject to seizure for the following reasons, which can also constitute a search:

- It is an instrument of a crime (i.e., used to make a call to execute a ‘hit’ on someone)
- It is a fruit of a crime (i.e., stolen good)
- Mere evidence of a crime (i.e., contains a video of a murder)
- Contraband (something illegal in its own right, like a stolen government computer or sawed off shotgun)

(Del Carmen and Hemmens, Chapter 7, 2015).

It is important to note, though, that while both a search and seizure are separate actions, both 1. need probable cause and 2. can happen incident to one another. A seizure can follow a search and a search can follow a seizure; However, in both cases, a search warrant is needed, as for a device being seized and searched.

SEARCH WARRANTS AND THEIR SCOPE

Search warrants define what can be searched for, and implicitly, that defines the scope of the search. A warrant is always needed when searching devices, no matter the scope of the search. When it comes to searching for property in the physical world, the rule of thumb used is: "It is unreasonable for a police officer to look for an elephant in a matchbox." (Del Carmen and Hemmens, Chapter 7, 2015). If the search warrant is for a 60-inch flatscreen TV, there is no need to be opening dresser drawers or kitchen cabinets in someone's home. This rule, however, is not as applied and understood in the digital world.

Recall that probable cause is needed to justify the legality of a search. Despite that, there are exceptions to warrantless searches, or those minimally invasive searches that do not require a warrant, like a frisk. A frisk is done only if the officer has reason to believe he or she is in immediate danger, like the suspect's possible/known possession of a weapon. A search involving the use of metal detectors and body scanners is also subject exception (to be later covered) (Del Carmen and Hemmens, Chapter 7, 2015).

FOURTH AMENDMENT EXEMPTIONS RELEVANT TO TECHNOLOGY

One exemption to the exclusionary rule would be special needs searches which "allows warrantless searches and searches on less-than-probable cause in cases where there are needs to be met other than those of law enforcement, such as the supervision of high school students, probationers, and parolees." (Del Carmen and Hemmens, Chapter 7, 2015)

Consider the use of technology in conducting special needs searches that would violate our privacy: the use of metal detectors in schools and x-ray searches of bags and luggage by TSA at the airport airports to assure the absence of weapons and contraband; the use of ankle monitors on probationers and parolees to track their location; etc.

Administrative searches, on the other hand, are used more for government regulatory compliance by government investigators. They are usually authorized by "local ordinances or regulations of administrative agencies and are generally conducted by agents or investigators of these agencies" and require a warrant. However, they are *not* to be used for gathering evidence to be used in a criminal prosecutions (Del Carmen and Hemmens, Chapter 7, 2015). In recent years, SCOTUS has had to firmly define the narrow exception to the allowance of warrantless administrative searches:

> "*One recognized exception to this requirement permits warrantless administrative inspections of businesses operating within certain industries subject to pervasive governmental regulations*." (*Mitchell v. Wisconsin,* 588 U.S. ___ [2019]).

Consider the use of administrative cell phone searches by employers. Would a warrant be needed if the device were a personally owned device or corporate device? If not, should warrants be required for these searches?

Keeping these different types of warrantless searches in mind, the circumstances in which technology can be used to conduct warrantless searches or be the subject of warrantless searches are often difficult to interpret and unique in a case-to-case basis, as later discussed in whether we have a REP of employer-owned devices.

THIRD PARTY DOCTRINE (TPD)

The TPD has been the center of modern debate regarding technology's implications in the Fourth Amendment. According to the American Bar Association (ABA), it is a judge-made rule that came about in *United States v. Miller* in 1976 (Arango, 2019) but was unofficially applied 3 years prior in *Couch v. United States*; both cases dealt with financial records and similar holdings by SCOTUS:

> "*The Supreme Court held that by disclosing financial records to an accountant or financial institution, a person no longer has a reasonable expectation of privacy in that information.*" (*Couch v. United States,* 409 U.S. 322 [1973]).

The TPD reduces our REP but does not eliminate it completely (Hayes & Kesan, Chapter 11, 2019). Our REP is reduced upon sharing information with a third party, implying that when we do this, we understand that this information can be turned over to the government without our knowledge and used in investigations- only the third party, then, is to be asked permission to turn over *our* information (Donohue, 2017). There are, however, limits to the TPD's application, as demonstrated in *Carpenter* with CSLI.

LITERATURE REIVIEW

In our modern world, emerging technologies are becoming increasingly central to our everyday lives. From the SHDs we have in our private residences to the devices we use in the workplace, the evolution of government regulation is still occurring. It is important we understand how these use cases impact our REP and what we can do to protect ourselves.

First, "the Fourth Amendment in a Digital World" by Laura Donohue, a professor at the Georgetown School of Law, provides the foundations for this paper. Next, Grace Manning's "the Third Party Doctrine in the Age of the Smart Home" examines REP implications of SHDs like Amazon's Alexa concerning the TPD. Then, this paper analyzes Marc McAllister's "Cell Phone Searches by Employers" article for a workplace-application of a REP.

THE FOURTH AMENDMENT IN A DIGITAL WORLD

Lauren Donohue's article on "The Fourth Amendment in a Digital World" examines how has technology been "challenging formal distinctions in Fourth Amendment doctrine" over the past century as technology began its bounding and exponential advancements that left SCOTUS overwhelmed with cases concerning technology and Fourth Amendment applications.

Donohue defines the root of the problem being the evolution of technology, the digitization of all aspects in life, including our privacy, and how lack of Fourth Amendment precedent in this territory is blurring the distinctions of legal dichotomies. How the pervasiveness

of information being collected and accessible by the government is more and more involved in the "intimate details of an individual's life" (pg. 573).

The scope of the article is wide, covering all major SCOTUS cases that involved Fourth Amendment run-ins with technology and privacy. Donohue focuses on four dichotomies that are "breaking down in light of new and emerging technologies": private vs. public space; personal vs. third party data; content vs. non-content; and domestic vs. international boundaries.

She additionally uses the writings of Justices to further enforce the dichotomies with occasional reference to evolving legal definitions in historical legal dictionaries.

While a strong inspiration for this paper, this article summarizes some case law about the implications of emerging technologies on the Fourth Amendment. In addition to the definitions and outside sources, it will be the main source for reference of case law regarding issues in the discussion section. Donohue reminds us that the Fourth Amendment was made for a physical world with physical things. The cases SCOTUS has seen at the time of their occurrence has produced some opinions that are departing in nature, especially currently, like in *Kyllo v. United States*.

In this case, Kyllo was suspected of growing marijuana in his garage. Government authorities did not obtain a warrant to search his home, so they used thermal-imaging technology to gather the heat signatures radiating off his garage to further support their suspicions. In the majority opinion, Justice Scalia wrote that "the surveillance is a 'search' and is presumptively unreasonable without a warrant." (*Kyllo v. United States,* 533 U.S. 27 [2001]). Of course, there is a large majority disagreeing with this opinion, as it departs from the norm of expected REP violations; but technology provides new avenues for searches every day nonetheless.

(Donohue, 2021).

THIRD PARTY DOCTRINE IN THE AGE OF THE SMART HOME

The Georgetown Law "Alexa, Can You Keep a Secret? Third Party Doctrine in the Age of the Smart Home" article written by Grace Manning provides a concise connection between the TPD, REP, and SHDs such as Alexa and Google Home.

Primarily, Manning focuses on the TPD implications of REP concerning Amazon's Alexa, perhaps the most well-known and used SHD. She mentions SCOTUS cases such as *Carpenter* and *Katz* in addition to two cases that involve Alexa herself. Whoops, I meant *itself*.

She details two instances where Alexa recordings were requested from Amazon by local law enforcement to help prove two murderers guilty to exemplify the lesser burden of proof. Not probable cause, but *reasonable grounds* that someone committed a crime and or did something wrong. The totality of circumstances used to establish reasonable grounds to obtain the recordings would need to convince a reasonable person (think, your average citizen) that a crime was committed.

The TPD has been involved in a handful of SCOTUS cases. Most notably, Manning writes that in *Carpenter,* the Court "declined to extend the third-party doctrine to data gathered by cell phones (Cell-Site Location Information (CSLI))" due to their "immense storage capacity" and "necessity to modern life", including their potential to expose the "intricacies of intimate activities" as seen in *Kyllo v. United States*.

"Do we have a REP in homes with smart home devices?" is the main question at hand here. Already, *Carpenter* does not allow the TPD to extend to exclusively cell-phone generated data, like CSLI; however, we use many third-party applications on our devices for different tasks, like Meta-owned social media platforms and shopping with Amazon or Ebay; Or, we connect our phones to non-TPD protected devices: SHDs.

Recall that SHDs sit in our homes, the most intricate places we reside in. They are constantly listening for 'trigger' words, which means they are on 24/7, feeding data back to their parent company. Sure, no person is guaranteed to be listening at all times, but these devices can also be vulnerable to intrusions by other third parties such as malicious hackers. One's REP is threatened by its very existence.

Manning argues that the TPD *should* extend to SHDs as well as the complete "nixing" of the doctrine entirely in turn for something more "robust" and modern to replace it.

Manning writes that the TPD originated from "..the idea that the law does not protect one who relays information to a trusted accomplice who later betrays him." In a modern application, though, the 'trusted accomplice' is the third party such as Big Tech companies like Amazon that can turn over the information without our permission to the government with a lower burden of proof than probable cause.

(Manning, 2019).

CELL PHONE SEARCHES BY EMPLOYERS

This article details both private and public cell phone searches by employers and their legality in accordance with the Fourth Amendment and SCOTUS cases.

Marc McAllister wrote “Cell Phone Searches by Employers” to address the current constitutionality of cell phone searches by both public and private employers in the workplace and whether employees have an REP, depending on what type of device they use (employer owned or employee owned, Bring Your Own Device (BYOD)). It is centered around the following two variables: “(1) whether the employee whose cell phone is searched works for a public or private employer, and (2) whether the cell phone is owned by the employer or employee”.

In addition to that, it also considers the workplace exception established by the SCOTUS *O’Connor v. Ortega* case in 1987 which “allows for certain employer-initiated searches on the basis of an employer’s own determination of reasonable suspicion”. Other SCOTUS cases such as *City of Ontario v. Quon* and *Riley v. California* have also addressed this matter in similar aspects, both of which have set precedent for employer cell phone searches of employer-owned and privately-owned devices respectively.

McAllister analyzes cell phone searches of employer-owned and privately-owned devices by public and private employers to establish “a framework for analyzing cell phone searches by employers” in three steps to be used in court:

1. Determine if the searching party acted within its capacity as an employer, and if that employer is a private or public employer.
2. Depending on the contents being searches, the court should determine whether the employee had an REP based on the following factors:

a. The employer committed an unauthorized intrusion or prying into the employee's seclusion.
b. The intrusion would be highly offensive or objectionable to a reasonable person.
c. The matter intruded on was private.
d. The intrusion caused the employee anguish and suffering.

3. If an employee's REP was valid, the court should determine the whether the search was "unreasonable for a public employer's actions" or "highly offensive for a private employer's actions" depending on the type of employer.

This article will be relevant in discussing how the impact of technology affects our Fourth Amendment REP protections in the workplace in addition to the workplace exception. (McAllister, 2021).

DISCUSSION

Our right to privacy may be an implied right in the Bill of Rights, but it is perhaps one of the most important rights Americans feel they have, but do not adequately understand. Our REP is also a difficult concept to understand, especially in modern times in a world of technology. This means it has many implications, some of which have been covered by the supreme court, as seen in *Katz* and *Carpenter*. But there are more REP applications: the TPD regarding SHDs and when public and government employees have a REP using corporate-issued mobile devices (CIMDs).

SMART HOME DEVICES, THE THIRD-PARTY DOCTRINE, AND OUR REASONABLE EXPECTATION OF PRIVACY

Recall that the TPD is a judge-made rule that came about from SCOTUS rulings *Couch* and *Miller* in the 1970s. In both cases, financial records disclosed to an accountant or financial institution were involved (Hayes & Kesan, Chapter 11, 2019). It did, at the time make sense to create an exception to the Fourth Amendment when "A suspect willingly disclosed information to a third party" in the case that there was fraud or embezzlement evidenced in those records. The world the TPD was made for, however, was not as technologically advanced nor was it imagined to be. Now, the TPD can be applied to many situations where we disclose information to a third party- something we do nearly every day and is becoming a necessity. Should we nix the TPD or modify it?

It is understandable that the TPD is important in the sense that the Internet is used as a component in nearly all crimes and that "wrongdoers could use third-party services in a tactical way to enshroud the entirety of their crimes in zones of Fourth Amendment protection." Just about anyone can enjoy the REP in the content of their messages, including criminals, which creates a burden for law enforcement to meet to get a search warrant for those contents. In order to get a search warrant, law enforcement uses the TPD to gather evidence from Internet Service Providers (ISPs) and Cell-Phone Service Providers (CSPs) with subpoenas and court orders that do not require probable cause, a lower burden of proof (Kerr, 2009).

Third party companies such as ISPs and CSPs are either subpoenaed or court-ordered for customer information needed by law enforcement. It is important to note, though, that a search warrant is needed for the content of communications unless they are older than 180 days. For this matter, the government can still obtain a search warrant, or 1. Get a subpoena or 2. Get a "specific and articulatable facts" court order, both of which require prior notice to the subscriber or customer (Kerr, 2004). These provisions of the Stored Communications Act (SCA) of 1986 would not be possible without the TPD.

Stored communications aside, the TPD can still be used to gather very private communications that are not considered content and can be obtained with a subpoena, court order, or search warrant. As seen in *Carpenter*, CSLI can be very revealing to one's private life and routines when gathered over long periods of time, despite it not being content (*Carpenter v. United States*, 585 U.S. ___, 138 S. Ct. 2206 [2018]). There is also the TPD implication that implies that for those who are not residents in a home, like visitors, have no REP. This was demonstrated in one murder case mentioned in Manning's article, *Arkansas v. Bates*; However, when law enforcement came to Amazon with a search warrant for Alexa recordings on the night

of the murder, Amazon refused to comply, citing a violation of *First* Amendment rights (*State of Arkansas v. Bates*, 370 U.S. 2 S. Cr. [2016]). How could Alexa have been listening, though? There are some triggers Alexa and other SHDs have in place to record potential domestic violence situations (Manning, 2019).

As seen in "Alexa, Can You Keep a Secret?", the TPD's application to SHDs and smart phones has high potential for abuse (Manning, 2019). It seems that on a case-by-case basis, though, its application to incredibly intimate third-party information is granted or suppressed: in *Carpenter*, the majority held that CSLI was information not applicable to the TPD, especially when considering the voluntary exposure rationale; recall that the TPD applies to information *voluntarily* shared with third parties. Applying the rationale to CSLI was seen as non-realistic by the Court, due to the pressing need for cell phones in everyday life and the near-to-none involvement of the customer in the generation of CSLI records beyond powering on the phone; However, three of the dissenting Justices of the Court wrote that CSLI still counts as business records and therefore does not circumvent the TPD (*Carpenter v. United States*, 585 U.S. ___, 138 S. Ct. 2206 [2018]).

The line technology draws for a REP has become blurred. Recall that a REP is an important component of the Fourth Amendment and its protections, a foundation for our right to privacy. Manning writes, "Given the rapid evolution of smart home technology, it is hardly a rare case where such privacy interests in third party records exist. Smart home devices will soon become a practical necessity of modern life." (Manning, 2019). The same is true for our cell phones: they are "such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society." (*Riley v. California*, 573 U.S. 373 [2014]) (*Carpenter v. United States*, 585 U.S. ___, 138 S. Ct. 2206 [2018]). Without a doubt, we use

these devices every day, the idea of ‘opting out’ of technology a laughable one. Our phones create extensive CSLI logs mapping out our travels while our SHDs perch upon our counters, at our beck and call as we ask them about today’s weather.

Our home is our most sacred and intimate space; by allowing SHDs to always listen to all our conversations knowing that what we say is recorded by Alexa and used, in say, targeted advertising (Iqbal et al., 2023). Congruently, our phones are becoming of equal depth and personally furnished as our physical homes and deserve similar TPD protections, too. Thus, the TPD should rather be modernized and modified accordingly to account for the many implications of various technologies it can be applied to.

CORPORATE-ISSUED MOBILE DEVICES AND THE WORKPLACE: WHEN DO PUBLIC AND GOVERNMENT EMPLOYEES HAVE A REASONABLE EXPECTATION OF PRIVACY?

Increasingly, we are beginning to use mobile devices in nearly every aspect of our lives including the workplace. Businesses have benefitted immensely from introducing mobile devices into their operations: better communication opportunities by eliminating the need for face-to-face meetings; better flexibility for those travelling; business processes can become automated or done outside the workplace; increasing productivity and efficiency; the list goes on (Sheldon, 2019). In the long run, this saves businesses money. When it comes to mobile devices, there are mainly two options for businesses: corporate-issued mobile devices (CIMDs) or Bring-Your-Own-Device (BYOD). Notably, BYOD policies have created controversy for business use

concerning their security and privacy implications. CIMDs also have these implications, too. When do public and government employees have a REP concerning their CIMDs?

It is first important to distinguish the difference of both types of policies. CIMDs are those mobile devices already purchased, vetted, and equipped with corporate policies and controls by the business exclusively dedicated for workplace use. In lieu of an employee termination, the business is returned the device to wipe and restore to its baseline for the next employee to use. As for BYOD, the business does not provide employees devices and request they perform necessary work operations on their personal mobile devices. To manage devices, businesses typically deploy a Mobile Device Management (MDM) application that enables them to monitor all company activity on those devices. Imaginably, this may be difficult to enforce in a BYOD setting (Schwartz, 2022) (Sheldon, 2019).

Both CIMD and BYOD have their benefits and costs when compared to one another. Most paramount is security and privacy implications. With CIMD, the security of mobile devices is more manageable especially with an MDM. Thus, the business is in full control of the mobile device's security controls and permissions (Schwartz, 2022). As for privacy, the Fourth Amendment exception of administrative searches creates a new concern. Also referred to as the pervasive-regulation exception, this means "administrative agencies can conduct warrantless searches of businesses attached to industries that have a long history of pervasive regulation." (Valbrune, et al., 2019). Generally, public and government employers cannot authorize the search of personally owned business devices without a warrant unless their policy defines very specific factors and circumstances for those situations although it would be best to obtain a warrant.

For CIMDs, a REP is generally lower, but still present. Employers, both public and government, are required to limit the scope of their search accordingly to be very specific

regarding the places to be searched and the information sought to avoid any Fourth Amendment REP violations. This was introduced by SCOTUS cases *O'Connor v. Ortega* and *Ontario v. Quon* (McAllister, 2021).

In *O'Connor*, the question of whether public sector employees had a REP of their private property in the workplace regarding government searches was raised. Justice Scalia, writing the majority opinion, concluded that government employees- or any public sector employees subject to regulatory searches -had a REP concerning their closed drawers and the files within them. If the government wanted to open drawers and see files, they would need a search warrant (*O'Connor v. Ortega*, 480 U.S. 709 [1987]). The same can be applied to CIMDs and BYODs; think of the mobile device as the drawer and its contents as the files.

Similarly, this concept was demonstrated in *Quon*; However, in this case, the mobile device in question was a pager that was warrantlessly searched for workplace misconduct, a search determined to be reasonable. Quon had acquired the pagers to use for his job as a police officer. The service provider charged extra every month for each time a pager exceeded the allowed character limit regarding texts. Quon had exceeded his monthly limit multiple times and thus his pager habits we investigated by the Ontario Police Department (OPD) which involved a warrantless request and search of those messages from the service provider. The Court acknowledged Quon's REP as valid, but for the case of workplace misconduct-related searches, it was not. Had they warrantlessly searched his pager if Quon did not exceed the monthly limit multiple times and did not have a workplace misconduct-related reason, Quon's REP likely would have been valid (*Ontario v. Quon*, 560 U.S. 746 [2010]).

With these cases in mind, it is evident that the REP of CIMDs is a slippery slope. Despite what business policy may say about employees' CIMDs, a REP is and will always be present, no

matter how infinitesimal. Nevertheless, employees cannot make an intrusion claim if "they have no reasonable expectation of privacy in the first place." (McAllister, 2021) (*O'Connor v. Ortega,* 480 U.S. 709 [1987]). Additionally, McAllister outlines 3 factors concerning a REP of privacy in an employment context:

1. The owner of the property is subject to intrusion.
2. Was the employee notified of the search, and did they consent to the search?
3. Was the property widely accessible or only accessible by the employee?

While there are also other important factors to consider, these questions are important to determining the context for establishing or dissolving a REP. *O'Connor* and *Quon* are both examples that support the idea that employee's REP should be carefully examined on a case-by-case basis. The "comingling of personal and work-related information" can occur in CIMDs, too, which also creates implications for searches of these devices (McAllister, 2021). Overall, it is best to assume that CIMDs have a restricted REP and that the device solely be used for work-related activity and nothing else. Company policy that outlines specific situations where employees' REP is diminished, like administrative searches, should be adequately developed and readily available to employee. This should include those cases where personal information like Personally Identifiable Information (PII) must be on the device as well as restrictions in place for search scopes that may interact with employee PII.

LIMITATIONS

The progression of our REP protections is largely dependent on the progression of emerging technologies and their growing application to everyday life, such as in our homes as SHDs and in the workplace with BYOD an CIMD policies. While there are a large handful of SCOTUS cases regarding technological implications of our REP, there are still new situations to be considered and new arguments to be heard, especially ones discussed here.

FUTURE RESEARCH

There is high potential for future research of this topic, some being in other applications of our REP and emerging technologies. As the years pass, new SCOTUS cases are heard and decided, new legislation on technology that may affect our Fourth Amendment rights, and new applications of technology are made that introduce new REP implications and violations.

CONCLUSION

The future of technology is forever promising, but the future of Fourth Amendment protections impacted by technology is vague. Like our right to privacy, Fourth Amendment

protections to some degree are embedded in everything we do, intertwined with the increasing and innate presence of technology. Where we use technology, we have some degree of REP, no matter how infinitesimal. From the devices in our homes, listening for the slightest of vocal cues to the devices we use in the workplace. Technology, while endlessly useful, threatens our right to privacy. We must understand that in many applications, we trade our privacy and experiences in life for the conveniences of technology.

Right now is a time of urgency. The pace is still fast, yes, but with the blink of an eye, it will be too late. It is vital to educate ourselves and others on what it means to have a REP and how technology implicates our privacy. The more people become aware of this right, the more power we will have in creating a voice to protect ourselves.

REFERENCES

Arango, Steven. Jun 13, 2019. "The Third Party Doctrine in Wake of a "Seismic Shift"." *American Bar Association.* https://www.americanbar.org/groups/litigation/resources/newsletters/privacy-data-security/third-party-doctrine-wake-seismic-shift/.

Boyd v. United States, 116 U.S. 616 [1886].

Brinegar v. United States, 338 U.S. 160 [1949].

Carpenter v. United States, 585 U.S. ___, 138 S. Ct. 2206 [2018].

Couch v. United States, 409 U.S. 322 [1973].

Del Carmen, Ronaldo; Hemmens, Craig. 2015. *Criminal Procedure: Law and Practice, Tenth Edition, Chapter 3: Probable Cause and Reasonable Suspicion. Cengage Learning.*

Del Carmen, Ronaldo; Hemmens, Craig. 2015. *Criminal Procedure: Law and Practice, Tenth Edition, Chapter 7: Searches and Seizures of Things. Cengage Learning.*

Donohue, Laura. 2017. "The Fourth Amendment in a Digital World." *Georgetown University Law Center.* https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2804&context=facpub .

"Fourth Amendment." N.d. *EPIC.Org*. Electronic Information Privacy Center (EPIC). https://epic.org/issues/privacy-laws/fourth-amendment/ . Accessed 13 Oct. 2023.

"Fourth Amendment." N.d. *Legal Information Institute (LII)*. Cornell Law School. www.law.cornell.edu/wex/fourth_amendment . Accessed 09 Oct. 2023.

Hayes, Carol; Kesan, Jay. 2019. *Cybersecurity and Privacy Law In a Nutshell, Chapter 11: Privacy Theory and Investigationsl. West Academic Publishing*.

Iqbal, Umar**;** Bahrami, Pouneh Nikkhah; Choffnes, David; Cui, Hao; Dubois, Daniel; Gamero-Garrido, Alexander; Markopoulou, Athina; Roesner, Franziska; Shafiq, Zubair; Trimananda, Rahmadi. Oct 13, 2023. "Tracking, Profiling, and Ad Targeting in the Alexa Echo Smart Speaker Ecosystem." *Proceedings of the 2023 ACM Internet Measurement Conference*. Cornell University. https://arxiv.org/abs/2204.10920

Katz v. United States, 389 U.S. 347 [1967].

Kerr, Orin. 2004. "A User's Guide to the Stored Communications Act." *George Washington Law Review.* Vol. 72, No. 26, pps 1208-1244. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=421860

Kerr, Orin. 2009. "The Case for the Third Party Doctrine." *Michigan Law Review.* Vol. 107, No. 4, pps 561-600. https://repository.law.umich.edu/cgi/viewcontent.cgi?params=/context/mlr/article/1348/&path_info= .

Kyllo v. United States, 533 U.S. 27 [2001].

Manning, Grace. 2019. “Alexa, Can You Keep a Secret? The Third Party Doctrine in the Age of the Smart Home.” *American Criminal Law Review.* Vol. 56, Winter Issue. https://www.law.georgetown.edu/american-criminal-law-review/wp-content/uploads/sites/15/2019/02/56-O-Alexa-Can-You-Keep-a-Secret-The-Third-Party-Doctrine-in-the-Age-of-the-Smart-Home.pdf .

McAllister, Marc. 2021. “Cell Phone Searches By Employers.” *Nebraska Law Review.* Vol. 99, No. 5, Article 4. https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=3301&context=nlr .

Mitchell v. Wisconsin, 588 U.S. ___ [2019].

O'Connor v. Ortega, 480 U.S. 709 [1987].

Ontario v. Quon, 560 U.S. 746 [2010].

Riley v. California, 573 U.S. 373 [2014].

Schwartz, Karen. Jun 28, 2022. “BYOD vs. Corporate-Issued Smartphones: Which Is Better for Small Business?” *Samsung Business Insights*. Samsung. https://www.insights.samsung.com/2022/06/28/byod-vs-corporate-issued-smartphones-which-is-better-for-small-business-3/ .

Sheldon, Robert. Sep 23, 2019. “Advantages and Disadvantages of Mobile Devices in Business.” *TechTarget*. https://www.techtarget.com/searchmobilecomputing/feature/Discover-the-benefits-of-mobile-devices-in-the-enterprise .

State of Arkansas v. Bates, 370 U.S. 2 S. Cr. [2016].

“U.S. Constitution - Fourth Amendment.” N.d. *Library of Congress*. https://constitution.congress.gov/constitution/amendment-4/ . Accessed 09 Oct. 2023.

Valbrune, Mirande; Cardell, Suzanne; De Assis, Renee; Mitchell, C. M.; Mitchell-Phillips, Kenneth; Sappleton, Natalie; Tayor, Tess. Sep 27, 2019. *Business Law Essentials I. OpenStax*. Business Law I Essentials - OpenStax