The Intersection of the Fourth Amendment and IoT

Jessica McMinn
5/7/2019

Table of Contents

Introduction

"Alexa, what's the best way to cover up a murder?" is what the Arkansas District Attorney expected to find on the Amazon Echo owned by James Bates. The case of Arkansas v. James Bates brought privacy and Fourth Amendment concerns to light at the end of 2017. As part of this case, the police served a warrant on Amazon for any recordings or transcripts of recordings in the 48 hours surrounding the alleged murder in hopes that the Echo present in the home would have picked up relevant evidence to the case. While Amazon mainly raised concerns over First Amendment rights in their Motion to Quash, the nation and media outlets quickly realized the alarming possibilities that Amazon's compliance with this warrant would have on the future course of privacy under the Fourth Amendment. This case opened consumer's eyes to the fact that yes their Echo speaker is always listening to and recording their conversations and that the existence of this technology changes the way people's privacy is protected and the meaning of that privacy.

While consumers were right to be concerned about the devices within their home that are by nature always recording their conversations, the perhaps more invasive aspect of smart home interconnectivity was largely ignored. In Bates' case, the records off his smart water meter were subpoenaed as part of the evidence. These water records showed that between 1am and 3 am on the night of the alleged murder 140 gallons of water were used which exceeded all other periods of water usage since October 2013 (Wang, 2017). This evidence was used to suggest that Bates was hosing blood off his porch between 1am and 3 am on the night in question.The disregard for Bates' privacy rights in this sense is even more apparent under the realization that the utility company instated a blanket installment of smart water meters on the homes they serviced (Wang, 2017).

As the Internet of Things (IoT) is becoming more prevalent in our daily lives, the need for security and privacy protections increases. The interconnectivity of the smart home creates a constant stream of private data about the current state of the home to large corporations with many access points for the government or hackers. Data collected by IoT devices is so deeply probative into people's daily lives that it can reveal intimate details like whether or not someone is inside the house, even including identification of that specific person and their physical location inside the house. Vulnerabilities in IoT such as these bring up a host of legal issues regarding the collection, transfer, storage and access to the subsequent data. Major issues as part of IoT arise under people's right to privacy and include aspects such as: the ownership of the collected data, the user's reasonable expectation of privacy, the breadth of the third party doctrine and overbroad requests for data under this doctrine.

This paper aims to examine the legal gray area regarding the use of IoT specifically within the house and the relation between searches and seizures of data collected by IoT devices and the Fourth Amendment. While this paper is not an exhaustive explanation of all laws governing IoT, it will help to place this new technology within the frame of outdated laws and ultimately argue that, with extremely probative devices operating with IoT, there needs to be a heightened recognition of individual privacy over the government's interest in gathering valuable evidence. To make these explorations and arguments, this paper will start by examining the evolution of case law regarding Fourth Amendment rights, then discuss the evolution of IoT technology specifically for devices commonly used within the home, and finish with an analysis of the law in relation to IoT.

Privacy and the Third Party Doctrine - The Evolution of Law

In order to let this examination build upon itself, the pertinent cases will be examined in chronological order. To complete this analysis, eight cases will be examined to determine the legal holding that followed the ruling on each case. As the US is based on a common law system, the holdings in these cases create legal precedent and laws in and of themselves to clarify the holdings of statutory laws.

Katz vs. United States

When discussing privacy rights particularly within the home, Katz vs. United States from 1967 is a good jumping off point seeing as the legal test from Katz is still used today when examining privacy cases.This landmark case arose due to Charles Katz's use of a public telephone booth to transmit gambling information to clients in other states. FBI operatives suspecting Katz of engaging in these illegal activities attached an eavesdropping device to the outside of the public phone booth to wiretap his conversations. His indictment based on these recordings led to the ultimate legal questions of "Whether a public telephone booth is a constitutionally protected area," under the Fourth Amendment and "Whether physical penetration of a constitutionally protected area is necessary," for a search and seizure to exist (*Katz v. United States,* 1967*).*

In deciding this case, the Supreme Court expressed that the questions asked by the petitioner (Katz) were not the relevant questions to be answered from this case because "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area'" (*Katz v. United States,* 1967). In moving away from the phrasing of "constitutionally protected area," the Supreme Court made a transition from the

previously property-based interpretations of the Fourth Amendment to what is now referred to as the "Reasonable Expectation of Privacy test."

The main opinion of the Supreme Court argued that the Fourth Amendment is intended to "protect people, not places" (*Katz v. United States,* 1967*).* The distinction made in this case by the Supreme Court is that regardless of place, the importance in determining Fourth Amendment violations is if the subject attempts to make something private versus publicly announcing that same information. In the case of Katz, he was using the protection of the phone booth to shield the contents of his conversation from the public and was in that sense relying on the privacy that the phone booth provided him.

The lasting impact from this case and the so-called reasonable expectation of privacy test, actually came from an alternate opinion on the case written by Justice Harlan. This test is a two-part test used to measure the subject's reasonable expectation of privacy as stated below (*Katz v. United States,* 1967).

1. An individual has exhibited an actual (subjective) expectation of privacy
2. The expectation is one that society is prepared to recognize as reasonable

Part one of this test shows that the subject has taken actual action to show that they are relying on the supposed privacy. For Katz, this action was taken by having his conversation inside of the phone booth. The mere action of having his conversation in an enclosed phone booth showed that he was using the phone booth for privacy and relying on its' ability to shield his words from the public. The second part of this test is significantly more objective than the first part in that society as a whole would agree that privacy in this instance is reasonable. In the case of Katz, it

was deemed reasonable by the court that society would accept that people should be able to rely on the privacy a phone booth affords to keep a person's conversation private.

In Katz's case and every subsequent case that does not have additional Fourth Amendment factors, this two part test has been used to determine the reasonability of a person's expectation of privacy in their particular setting. This test has become integral to Fourth Amendment cases as it dictated that in situations where a person has a reasonable expectation of privacy, a warrant was required to perform a search.

United States vs. White

Shortly after deciding on *Katz*, the Supreme Court had another case involving the Fourth Amendment in relation to informants. In United States vs. White, the issue of whether or not testimony from government agents who overheard conversations between the defendant and an informant, who was wearing a radio transmitter that the agents could receive transmissions from, would be admitted in court. This case dealt with many different forms of eavesdropping on the defendant. In total, there were eight different conversations that were overheard by law enforcement. With the help of Harvey Jackson acting as an informant, the agents were able to overhear conversations within Jackson's home where, with Jackson's consent, one agent was hiding in the house and another was listening outside with a radio receiver (*United States v. White,* 1971). The other four conversations in various places "were overheard by the use of radio equipment" aided by a radio transmitter concealed on Jackson's person (*United States v. White,* 1971).

In deciding this case, the court centered around the idea that a defendant does not and cannot have "a justifiable and constitutionally protected expectation that a person with whom he

is conversing will not then or later reveal the conversation to the police" (*United States v. White,* 1971). In short, this decision revolves around the idea that as soon as information is shared with someone else, the original person cannot have an expectation that the shared information will never be passed on, even to the government.

Under the eyes of the court, there is no difference between confiding in a police officer and confiding in someone while the police are listening. In this sense it does not matter who the person is or what their affiliation is, it only matters that the original person has shared their information with another and cannot prohibit that person from telling the police at a later time or immediately by way of electronic surveillance.

People assume the risk every time they open their mouth or engage in illegal activity that their colleagues or accomplices might be cooperating with the police. In deciding this case, the Supreme Court argued that a person who suspects their colleague of cooperating with the police would treat that person no differently if they suspected them of being wired or not. In short if a person suspects their colleagues of cooperating with the police that person already has no expectation of privacy of their conversations and that expectation of privacy would not be diminished whether or not the colleague was wearing a wire.

Smith vs. Maryland

Smith vs. Maryland is the next of pertinent cases and discusses the use of pen registers and regularly collected business records. In this case, defendant Smith was accused of robbing a woman and calling her at her house to threaten her. Police were able to spot the car she saw at the time of the robbery and trace it back to defendant Michael Smith. Using this information, the police requested that the phone company place a pen register on Smith's phone to record the

numbers dialed from his house. As the pen register was not placed under a warrant, it begged the question of if Smith had a reasonable expectation of privacy in the numbers dialed from his house and if a search had occurred under the Fourth Amendment. As the Court saw it there was a distinctive difference between *Katz* and this case in regards to a reasonable expectation of privacy. For *Katz*, the contents of his conversations were recorded, whereas "pen registers do not acquire the contents of communications" (*Smith v. Maryland,* 1979). The realization of this difference by the Court showed that, in their opinion, the intrusiveness of data collection matters as well as the purpose of collection for the lawfulness of a search.

Reasonable expectation of privacy is a determining factor for whether or not a search existed under the Fourth Amendment and the Supreme Court argues that "people in general [do not] entertain any actual expectation of privacy in the numbers they dial" (*Smith v. Maryland,* 1979). Going back in time to the origin of telephones, this reasoning makes perfect sense. When telephones were first invented, an operator was used to manually transfer the call and would ask the calling party to which number they would like to connect. If it is necessary to physically tell someone what number the caller would like to connect to, then it is clear that people do not really have any expectation that the numbers they dial are private. Although in today's automated age, there is no middle man doing the physical connecting, the phone company must be aware of what numbers are being called in order to place the call.

Furthermore, users recognize that the phone company must be recording their phone records in a permanent file in order to charge them for their calls. Today, most phone users have phone plans that include unlimited calls all over the US and can easily connect to other countries through Wi-Fi calling. Before this technology came into use, people were specifically charged extra for long distance calls which would come up on their monthly telephone bills, thereby

making consumers aware that phone companies were tracking their calls. In fact, phone companies were using pen registers regularly for the company to conduct their operations, properly bill their customers and detect fraud (*Smith v. Maryland,* 1979).

In arguing the case, petitioner argued that since the call was being placed from within his own home, he had a reasonable expectation of privacy. The Court argued that he could claim a reasonable expectation of privacy over the contents of the conversation which was not recorded but did not have any claim to privacy on the number dialed. Another explanation of this relied on the fact that this information was turned over to a third party and that once information is voluntarily turned over to a third party there can be no reasonable expectation of privacy.

There were several other interesting points brought up in this case came from the dissent of Justice Stewart and Justice Marshall. Justice Stewart argued that the number dialed was also part of the content of the call and should be protected as such (*Smith v. Maryland*, 1979). Justice Marshall argued the idea of "voluntary" in regards to people sharing their information with a company. Marshall claims that when there is no practical alternative to turning over information, it cannot be truly voluntary (*Smith v. Maryland*, 1979). In his mind, because people do not have a practical alternative to using a cell phone and therefore giving a phone company access to their call records, those records should be protected under the Fourth Amendment.

Advancement of the third party doctrine was also an integral result of this case. The Supreme Court holds that, following from their decision in United States vs. White, once information is shared with another party, it is no longer private and negates any claim to reasonable expectation of privacy. The Court specifically extended this to business records as it is typically referenced today, noting that "This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (*Smith*

v. Maryland, 1979). The third party doctrine has since grown from this point to mainly refer to people voluntarily giving their information to businesses such as banks, phone companies, internet service providers and email servers. In an ever more technological world, the third party doctrine has the opportunity to cover many more aspects of life and allow government entities to obtain these personal records from the third party without a warrant as people do not have a reasonable expectation of privacy over these records and the government's obtainment therefore cannot be classified as a search.

California vs. Greenwood

The case of California vs. Greenwood deals with a trash pull and the reasonable expectation of privacy a person can have on property that is outside the curtilage of the home. In this case, defendant Greenwood was suspected of drug trafficking. In order to gain evidence, police asked the trash collector to pick up the bags from in front of Greenwood's house and, without mixing them with any other bags, deliver them to the police. The police were able to go through Greenwood's trash and find enough evidence to get a warrant to search his house. However, the initial trash pull was done without a warrant which led to the question of whether or not a search violating the Fourth Amendment occured in Greenwood's case.

In deciding this case, the Court argued whether or not Greenwood relied upon a reasonable expectation of privacy that society was willing to recognize. While Greenwood had taken actions that "exhibited an actual expectation of privacy" by bagging his trash in opaque bags to shield the contents from public view, the Court argued that society was not ready to recognize his privacy as to the contents of his trash (*California v. Greenwood*, 1988).

The reasoning for this decision was due to the public nature of his trash. Reasoning given by the Supreme Court was that,

> "It is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public…. Moreover, respondents placed their refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so. Accordingly, having deposited their garbage 'in an area particularly suited for public inspection and, in a manner of speaking, public consumption, for the express purpose of having strangers take it,' respondents could have had no reasonable expectation of privacy in the inculpatory items they discarded" (*California v. Greenwood,* 1988).

While this case is very unique from the others in that it deals with physical property and does not deal with technology at all, it contains many key aspects of reasonable expectation of privacy and the third party doctrine. The Court used the fact that trash is left specifically for someone else to pick it up to argue that once the trash leaves the property of the owner, they no longer have a reasonable expectation over the privacy of that trash (*California v. Greenwood,* 1988). Because anyone can go through trash at will and steal it or search through for useable items, privacy does not extend once it leaves the curtilage of the house making a trash pull not a search under the Fourth Amendment.

Kyllo vs. United States

Plaintiff Kyllo under suspicion of growing marijuana inside his house prompted agents of the United States Department of the Interior to use an Agema Thermovision 210 to measure the heat emanating from his house (*Kyllo v. United States,* 2001). As high intensity lamps are used to grow marijuana, a large amount of heat is emanated and can be measured without having to go inside the house. Images coming from the Agema Thermovision 210 appear as heat images giving a blotchy appearance of the amount of heat in a certain area. This test was performed in a matter of minutes from the streets in front of the house and in back of the house, which meant that the agents did not have to step onto the physical piece of property, let alone into the house, to measure the heat signatures (*Kyllo v. United States,* 2001).

In deciding Kyllo, the Supreme Court further supported their decision in *Katz* by applying it to claim that a "search does *not* occur - even when the explicitly protected location of a *house* is concerned - unless "the individual manifested a subjective expectation of privacy in the object of the challenged search," and "society [is] willing to recognize that expectation as reasonable" (*Kyllo v. United States,* 2001) This was a direct move away from the Fourth Amendment as written which specifically protected places such as the house.

Under the *Katz* test, Kyllo had not only made no attempt to cover up the heat coming from his house and therefore had no subjective expectation of privacy. Additionally, the Ninth Court when reviewing Kyllo's case found that there would be no objective reasonable expectation of privacy since the Agema Thermovision 210 only showed "amorphous 'hot spots' on the roof and exterior wall" and these hot spots "did not expose any intimate details of Kyllo's life" (*Kyllo v. United States,* 2001). Upon review by the Supreme Court, the Court emphasized that "In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying eyes."

As the test of reasonable expectation of privacy under *Katz* was not helpful in this case, the Court looked for a new test to explain the privacy rights and turned to emerging technology. In a forward looking view, the Court recognized that advancing technology had a big effect on "the degree of privacy secured to citizens by the Fourth Amendment" (*Kyllo v. United States,* 2001). As an example of the diminishing privacy rights of citizens with the evolution of technology, the Court pointed to flight. Before airplanes and human flight were possible, it was reasonable for people to believe that "uncovered portions of the house and its curtilage" were private" but with new technology are now accessible to law enforcement since they are openly viewed by private and commercial pilots and passengers (*Kyllo v. United States,* 2001). As people become more able to use technology to access parts of ordinary life that used to be private, their lives are more easily captured by the government.

To decide how the discrepancies on technology should be considered, the Court incorporated *Katz'* test. As technology grows, people's objective reasonable expectation of privacy diminishes. In short, if a certain technology is widely used in society, then private citizens do not have a reasonable expectation of privacy to be free from the use of that technology. This brings the idea of objective reasonable expectation of privacy into the technological sphere. Overall, the evolution of technology led the Court to their decision that when the technology is not in "general public use" and it allows the government "to explore details of the home that would previously have been unknowable without physical intrusion" then the use of the technology is a search (*Kyllo v. United States,* 2001).

United States vs. Jones

In the evolution of the legal opinion surrounding the Fourth Amendment, the Court had held fast to the idea of reasonable expectation of privacy since its inception in *Katz.* The original wording of the Fourth Amendment is as follows:

> "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. Constitution).

The original phrasing of the Fourth Amendment refers to property specifically and safeguards tangible things. Post-Katz evolution of cases led the Court away from an interpretation of property and to the privacy of the person. Jones' case deals specifically with the search of personal records via infringement on personal property.

In this case, Jones, suspected of trafficking narcotics, had a GPS tracking device installed by agents on the underside of his Jeep. The agents tracked his every movement for a 28 day period that resulted in over 2,000 pages worth of data (*United States v. Jones,* 2012). In defense of this highly probative and intrusive amount of data, the Government looked to United States vs. Knotts and claimed that the *Katz* rule applied to traffic patterns because "[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). This argument coming from *Katz* continues the idea of reasonable expectation of privacy.

People's movement on public streets is open to observation by all users of the public road. Due to the open nature of this data, the Government argues that people cannot have an objective reasonable expectation of privacy in their movements. Therefore, the Court decided that the *Katz* test solely applied would uphold this search.

However, the Court points out in the wording of the *Katz* test that "We have embodied that preservation of past rights in our very definition of 'reasonable expectation of privacy' which we have said to be an expectation 'that has a source outside the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society,'" that it is inclusive by nature.

Katz test, the Court explains, is inclusive, not exclusive and was meant to add more protection, not change the factors of protection. It kept all of the original aspects of the privacy of property that is guaranteed under the Fourth Amendment and added on another framework to decide if additional privacy concerns were at stake. Under the wording of the Fourth Amendment with protection of a person's "effects" from unlawful searches, a car very much so falls into this category and its search would violate the Fourth Amendment (U.S. Constitution).

The Court explained that, "by attaching the device to the Jeep, officers encroached on a protected area" (*United States v. Jones,* 2012). By physically penetrating the vehicle and attaching a device even to the bottom of the car, "the government physically occupied private property," and infringed upon the private property of a citizen (*United States v. Jones,* 2012). Previously in *Class,* the Court had even noted that encroaching on a protected area would make a difference in deciding whether there was a lawful search or not (*United States v. Jones,* 2012).

Arguments on the Government side, show the confusion that was left after the *Katz* test came into play. Many other actors agreed with the Government's interpretation of *Katz* and

assumed that by the Court's reliance on this rule over time, it was meant as an entirely new interpretation of the Fourth Amendment and was the only factor necessary in considering a potential Fourth Amendment search. The Court took this opportunity to clarify once and for all that *Katz* was meant to be invoked only when there was no physical source clearly protected by the Fourth Amendment. Summarizing this point, the Court says that "situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis," as this type of trespass has no physical attributes (*United States v. Jones,* 2012).

David Leon Riley vs. California

Riley was stopped for driving with expired tags and had his car impounded upon that realization (*Riley v. California,* 2014). Under protocol, the police searched the car before taking it to be impounded and found that there were several concealed and loaded firearms in the car for which Riley was arrested (*Riley v. California,* 2014). Still within protocol, the officer searched Riley due to his arrest and found a cell phone in one of his pockets along with other items seemingly associated with the "Bloods" gang. The officer and another detective were then able to search through his phone and examine the contents for items pertaining to gang activity. In one of the pictures on his phone, he was standing in front of a car suspected of involvement with a previous shooting. He was ultimately charged for the crimes associated with the shooting, proof of which all stemmed from the pictures found on his phone from his earlier arrest.

The rule for determining the reasonableness of a search incident to arrest stems from Chimel vs. California where officers arrested Chimel inside his house and then proceeded to search his house. The Court gave the following rule to determine the reasonableness of a search incident to arrest:

> "When an arrest is made, it is reasonable for the arresting officer to search the person arrested in order to remove any weapons that the latter might seek to use in order to resist arrest or effect his escape. Otherwise, the officer's safety might well be endangered, and the arrest itself frustrated. In addition, it is entirely reasonable for the arresting officer to search for and seize any evidence on the arrestee's person in order to prevent its concealment or destruction… There is ample justification, therefore for a search of the arrestee's person and the area 'within his immediate control' - construing that phrase to mean the area from within which he might gain possession of a weapon or destructible evidence" (*Chimel v. California,* 1969).

Shortly after *Chimel,* another case came up dealing with unwarranted searches incident to arrest. *Robinson* dealt with searches of the arrestee's physical person. When Robinson was arrested for driving with a revoked license, his pat down revealed an unidentifiable object which turned out to be a crumpled cigarette packet that the officer opened and found heroin (*United States v. Robinson,* 1973). While this search was incident of an arrest and was deemed acceptable by the Government, it was very unlikely that the officer was looking for evidence of the crime or performing a search for their own safety when they found the heroin. However, the Court still held that when a person is arrested under probable cause, "a search incident to the arrest requires no additional justification" and that the officer was entitled to inspect things they came across during the search (*United States v. Robinson,* 1973).

In the case of Riley, his phone had been found during a regular search incident to arrest and had been found in an area under his "immediate control" which following past precedent

allowed the officer to inspect his phone. There is, however, a great deal of difference between a phone and a physical object. For starters, where phones are concerned, the risks found under *Chimel* are not important. Digital data stored on a phone poses no immediate real risk to an officer's safety and it can also not be destroyed easily. Even if officers were worried about data stored on the phone being destroyed, they could turn it off or place it in a Faraday bag to prevent the loss of data while they are waiting for a warrant. Because of the lack of these risks, it begs the question of if officers can inspect the data stored on cell phones as part of a warrantless search incident of arrest.

When looking at the search of data on cell phones, the Court recognized that there was no significant risk posed by the phone and that the data they could provide is extremely probative. Modern smartphones have a massive amount of personal data stored on them and can provide in-depth information on almost every aspect of a person's life. The Court noted that cell phones are not really cell phones anymore and they are "in fact minicomputers" that "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, or newspapers" (*Riley v. California*, 2014). Expressing the full array of functions of a smartphone notes the impracticality of claiming the ability to search a phone incident to arrest. Clearly, it is very unlikely that a person would be carrying around all of these items at the same time, thus making it impossible for officers to perform warrantless searches on all of these items at the same time incident to an arrest. Not only do phones contain quantitatively more data, but the quality of the data is much more revealing about a person's private life. Apps and internet records for example can reveal the sexual orientation, relative health, political affiliation and more of a person and be intensely probative in the amount of intimate information they contain.

On this issue, Learned Hand very aptly remarked in an opinion that would later be cited in *Chimel* that:

> It is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him" (*United States v. Kirschenblatt*, 1926).

The opinion of the Court noted that the amount of intimate data now stored on cell phones makes Hand's statement false "if his pockets contain a cell phone" and that a cell phone would in fact usually reveal "far *more* than the most exhaustive search of a house" (*Riley v. California*, 2014).

To further complicate the data stored on cell phones, there is also a significant amount of data that appears through the interface of the cell phone but is actually stored on the cloud. Most users are not aware which of their data is stored on the cloud, and to further complicate this, the data that a device stores on the cloud can in fact differ depending on the type of device These discrepancies along with the fact that the data is not technically on the device, and that almost every detail of a person's life can be accessed through cloud storage situate this data in a clear territory of needing a warrant to obtain access along with other cell phone data as per the Court's decison.

Carpenter vs. United States

The case of Carpenter deals again with the invasive nature of smartphones, but pertains specifically to historical data and the differences in the barriers to data access under the Stored Communications Act and warranted searches under the Fourth Amendment. Carpenter was

arrested along with three other men for a series of armed robberies. One of the men confessed and cooperated, giving the FBI his personal cell phone number and the cell phone numbers of his accomplices. The FBI then used these cell phone numbers to apply for orders from magistrates to obtain "transactional records" pursuant to the Stored Communications Act (*Carpenter v. United States,* 2018).

This act allows the government to require disclosure of telecommunication records when "specific and articulable facts show[] that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation" (The Stored Communications Act). Under this act, the Government only needs to prove that the records are important for an ongoing investigation, which is an extremely low bar compared to that of probable cause under the Fourth Amendment.

Not only is the barrier to access much lower under the Stored Communications Act, but the information requested by the Government was extremely invasive by nature. The Government requested cell-site data for Carpenter's phone which by triangulating calls works very similarly to a GPS and provided the Government with "12,898 location points cataloging Carpenter's movements over 127 days - an average of 101 data points per day" (*Carpenter v. United States,* 2018).

The Court argued that while this cell-site data is not physical property, it could fall under the idea of reasonable expectation of privacy from *Katz.* Generally, the Court has held that a reasonable expectation of privacy does not extend to information voluntarily shared with other parties under the "third-party doctrine". This doctrine was developed in United States v. Miller and *Smith.* In *Miller,* the Court held that documents that were part of a business's ordinary course

of business were not subject to a reasonable expectation of privacy because they were "not confidential communications" and were "exposed to [bank] employees in the ordinary course of business" (*United States v. Miller,* 1976). *Smith* provided that "voluntarily conveyed" information such as the number dialed to a phone company had no expectation of privacy as they were required for the company to conduct business (*Smith v. Maryland,* 1979). The Government in *Carpenter* made the same assertion in regards to cell-site data as it was required for the business of the cell phone company. Cell-site location data comes from the triangulation of cell towers and it is impossible for a phone company to place a person's call without knowing where the person is located.

The Court ultimately decided not the extend the third party doctrine to cell site data due to the intrusiveness of the new technology that the framers of the Constitution would have had no way of predicting. Additionally, the Court disputed the notion that cell-site data was voluntarily shared with third parties - which is a key feature of lack of reasonable expectation of privacy under the third party doctrine. The Court argued that "cell phone location information is not truly "shared" as the term is normally understood. First, 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. Second, a cell phone logs a cell-site record by dint of its operation" (*Carpenter v. United States,* 2018). Because cell phones are integral in daily societal life, and because they perform many functions that users do not affirmatively use let alone understand, they cannot be expected to be voluntarily giving that information away to a third party. Due to these distinctions between cell-site data on smartphones and the overall evolution of technology past what the framers of the Constitution could have imagined, the Court held that the Government will still need a warrant to access this data.

Legal Conclusions

There are two main takeaways from the progression of these cases. First, are the legal tests that have been and will continue to be used to determine when a search under the Fourth Amendment is occuring. If there is physical property being searched and it fits in one of the constitutionally protected areas: “persons, houses, papers, and effects,” then is is likely that the specific property is protected (U.S. Constitution).

Under *Katz* rule, there is another category of searches and that is when people have a subjective and objective reasonable expectation of privacy in their intangible items. This rule mainly pertains to electronic recordings. While the Court has mainly decided not to protect conversations and records as part of regularly conducted business, they have found massive amount of data easily collected and archived through the use of technology to be safe from unwarranted searches. Additionally, the Court has continually noted that technology is growing so rapidly that the old standards of the Constitution make it difficult to govern new technology and the legislature needs to write new laws. Because of this rapidly advancing technology, the Court has also argued that it is hard to say that people necessarily voluntarily give away all of their data transcribed on a smartphone because most people don’t understand how this technology works and how or where their data is stored.

Technological Background - Devices in the Smart Home

Our homes used to be relatively low-tech buildings. The addition of TVs and computers helped start a wave of increasing technology within the home. The homes we live in today are not only physically wired and interconnected, but through the advance of technology even mundane objects like lightbulbs can be connected to a user's phone to change color or turn on when you walk into the room. All of these devices that come together to create a smart home are typically connected via bluetooth and can be accessed through a smartphone and controlled via a home device like Google Home or Amazon Echo. This helps separate the big differences in devices within the smart home into two categories, voice activated and other IoT.

Voice Activation

Voice activation can come in two forms, the most common being always-on recording, and the other being recording that requires an outside signal to start recording ie the touch of a button. Devices that rely on an outside signal to record, will only record once that signal has been given. Always-on recording though requires the device to be constantly recording and processing data on some level at all times.

For devices that use always-on recording, the main functionality comes from the use of keyword spotting and large vocabulary continuous speech recognition software. Keyword spotting is what allows devices to constantly process all conversations while simultaneously conserving electricity and bandwidth, and providing an extra layer of privacy for the user. In order to remain low-cost and energy efficient, voice activated devices run on microcontrollers that "typically consist of a processor core, an on-chip SRAM block, and an on-chip embedded flash" (Zhang, Suda, Lai, & Chandra, 2018) . These systems have the entire neural network

model with input/output, weights and activations all typically contained within a maximum of a few hundred kilobytes (KB) of memory. The intensive processing they do within such a small framework leaves minimal storage for actual sound bites on the chip.

To keep energy consumption low and work within this framework, keyword spotting and large vocabulary continuous speech recognition (LVCSR) is used which allows the device to process a constant stream of speech while waiting to record until it comes across the device's pick-up word like "Alexa" or "Ok, Google". These systems essentially work like the reverse of a buffering system when watching streamed content. Small snippets of voice are constantly recorded, processed and analyzed for the keyword, momentarily stored and soon deleted if the keyword is not found (Zhang, Suda, Lai, & Chandra, 2018). Chart 1 provides a diagram of how this process works.

Once the on device processing picks up a keyword, the voice command following the keyword plus a small amount of the preceding voice recording that is stored on the device will be sent off site to the cloud for processing. The amount of preceding voice recording that is sent is typically very small as the microcontroller has a minimal ability for storage. For example, products that run on Amazon's Alexa Voice Services only send 500 milliseconds of proceeding voice (Amazon. *Requirements for Cloud-Based Wake Word Verification)*. The amount of information stored on the flash of the microcontroller and memory is typically heavily encrypted often with "hardware-based, single-or triple-DES algorithm," making the data stored on-device almost impossible to access (Bursky, 2011).

The sound bites and data collected by other IoT devices are also heavily encrypted when they are transferred from the device to the cloud. These sound bites are stored on the cloud and can be access through the user's account much like a person's Internet history. For example,

users of Amazon Voice Services can access their voice recordings through the Alexa app (Amazon. *Review Your Voice Recordings)*. To do this they can open their app and go through the following progression to find their recordings: Settings > Alexa Account > Alexa Privacy > Review Voice History. On this page they can find all of their past voice recordings following their chosen pick up word and a transcription of the exchange. They can also access recordings but not transcriptions of their past false pickups.

A false pickup happens when the device believes that it has heard the pickup word and sends the recording to the cloud to be processed. Upon reaching the cloud for processing, more advanced natural language processing software recognizes that it is a false pickup, does not transcribe the recording but keeps it in the database. Natural language processing software learns from having a large database and improves when it has a larger and more varied bank of user data. Using this metadata it can analyze and provide better responses to commands as well as learn to recognize its primary users. Due to privacy concerns, users are able to delete their past recordings through the device's Voice History page.

Privacy in the Smart Home

Smart devices within the home have multiple vulnerabilities to their protection and their privacy. Devices like these are subject to hardware and software holes that would potentially allow hackers to access the device and its data. In addition to these concerns as can be seen from the legal discussion above, it is unclear exactly how this data will be treated by law enforcement, the courts, and the government as a whole. To discuss all of these in turn, an exploration of the hardware and software vulnerabilities present in an array of devices used within the home will

start and then a discussion of how these devices and their information intersect with the Fourth Amendment will follow.

A Discussion of Devices - Voice Activated

When thinking of devices that have an ability to record and collect a large amount of data on users and their consumer habits, the first devices that come to mind are the "home" devices that act as a hub for other smart devices. Amazon Echos and Google Homes as well as other "home" devices act as a hub for other smart devices by directing and controlling what they do. For example instead of using a phone app to control the lights in a house, a user that has a hub like this can use voice commands to ask their hub to control the other smart devices. Due to this hub system, voice activated devices have a uniquely small attack surface compared to larger devices connected to the same network. Voice activated devices can only be compromised remotely by hackers through voice command or during the transfer of information from the device to the cloud (Montag, 2018). Compared to a computer or smartphone that are connected to the same home Wi-Fi network as a hub device, the opportunities for hacking into the network via a hub device are quite limited and make them not common targets to hackers who favor computers and smartphones. Additionally, each of these devices have specific software and hardware vulnerabilities due to their company's privacy policies and manufacturers.

Amazon Echo

Amazon Voice Services operating on Amazon's Echo devices use encryption to pass data from the Echo speaker to cloud processing and storage. In testing by AV Test, an Independent IT-Security Institute, it was found that all communications of the Echo used TLS 1.2 encryption

protocol and securely prevented simple man-in-the-middle attacks (Purche, 2017). A man-in-the-middle attack means that the hacker is able to insert themselves in-between the two parties while they still believe they are communicating with each other. They also found that no sensitive data was stored locally on the device outside of a protected storage area (Purche, 2017).

In their privacy policy, Amazon publishes that they collect, process and retain information on users' "voice inputs, music playlists, and your Alexa to-do and shopping lists" among other data points in the cloud (Amazon. *Alexa Terms of Use)*. These things should come as no real surprise to users of Amazon's service as these recordings are easily viewable on the Amazon Alexa App, and are communications that Alexa must collect in order to fulfill the requested task. Amazon also stores a user's messages in the cloud so they can be accessed through the Alexa App and allows auxiliary products to know the "device type, name features, status, network connectivity and location" of the device (Amazon. *Alexa Terms of Use)*.

As a hub system, it is quite common for devices such as these to share information with third parties. For example if a user asked for a weather report or for Alexa to play a custom playlist on a music service such as Spotify, these services would be a Third Party Service to Amazon Voice Services. In order for a user to enjoy the full range of possibilities of a smart speaker's hub system, the speaker must be able to communicate with third party services and share some consumer data. Imagine for example, asking Alexa to give a weather report without Amazon Voice Services being able to share the user's location with the weather app, this would be an obvious barrier to an accurate response. Amazon therefore, shares related information with the particular third party service even going so far as sharing telephone numbers with third party services providing communication services.

Google Home

The hub device released by Google, the Google Home, also runs with on-device keyword spotting and uses encryption to keep data private while in transit. As a whole, Google's policy of sharing data with affiliate partners is fairly open. Google will share device data with affiliate partners to collect information from a user's browser or device for advertising purposes and share relevant personal information with consent when asking for a service (e.g. sharing a user's name and phone number when using Google Home to make a restaurant reservation) (Google. *Privacy Policy)*. Google tries to generally only provide transcripts to third parties and not the actual voice recordings (Google. *Privacy Policy)*. This is important due to the amount of demographic information and security concerns that can be revealed through a voice recording. A person's voice is entirely unique and are increasingly being used as security features in lieu of passwords or other security measures. Voice can also reveal intimate details about a person such as sex, race and age. Google does make strides to restrict employee access to personal data and enforce "strict contractual confidentiality obligations" on the employees, contractors and agents who may have access to it (Google. *Privacy Policy)*.

As far as Google Home is concerned, the Home device has access to search and location history. If allowed, it will go through a user's search history with the goal of providing more helpful answers. It will also guess an approximate location based on the IP address if the user chooses not to provide their address while setting up the device. Location data is important for providing weather and traffic information as well as making sure the user's alarms are in the right time zone (Google. *Data security & privacy on Google Home)*. The conversations are encrypted and can be deleted at anytime through "My Activity" in the same way Amazon allows users to delete their Alexa voice recordings (Google. *Data security & privacy on Google Home)*.

Google Home shares data with third parties in an extreme way. It allows a third party service to "use information from past conversations with you, even if they happened on different Google Home devices" (Google. *Data security & privacy on Google Home).* While this "information" is hopefully the transcripts of conversations instead of the recordings and protects the intimate information discussed above, it certainly allows access to a wealth of information without direct consent of the user. As an attempt to ease these blatant privacy concerns, Google requires third party services to publish a privacy policy detailing what information they record, how they use it and how the user can control their use of the data.

Samsung Smart TV (remote)

The Samsung Smart TV remote is strictly meant as a touch-activated device. This separates it into an almost subcategory of the voice activated devices. It does not use on-device keyword spotting as it is meant to only record once the physical button is pushed. Using a push button, allows the user to be certain of what is actually being recorded unlike always-on technology that can have false pickups from time to time. For example if Alexa overheard a conversation about someone driving a Lexus, the device might falsely report "Lexus" as "Alexa" and start recording. While companies are working to reduce the prevalence of false pickups in their devices it still happens in always-on recording devices such as when Alexa recorded and sent a private conversation to a contact of the user (Chokshi, 2018). By requiring a physical touchpoint to start recording, the remote for the Samsung Smart TV helps safeguard over device error.

As far as Samsung's Privacy Policy for their Smart TV, they tailor content based on a user's zip code and collect data on: content users watch/download/stream, the applications they

access, the “Likes” and “Dislikes” users assign to programs, query terms put into the SmartTV search feature, IP address and browser information (Samsung. *Samsung Privacy Policy -- SmartTV Supplement).* Samsung uses a third party, Nuance Communications to process their voice services feature. This third party company has access to all voice recordings as they are responsible for converting the voice commands to text. Samsung also collects voice recordings to improve voice recognition (Samsung. *Samsung Privacy Policy -- SmartTV Supplement).* So while Samsung employs the more secure feature of physical touch for active recording, they share all voice recordings with a third party. There is also the possibility of using facial recognition as a security feature for the TV which stores the image locally without transmitting the image to Samsung (Samsung. *Samsung Privacy Policy -- SmartTV Supplement).*

All Recording Devices Considered

While each of these devices have their differences, there are some common characteristics between devices that are important to note. In a discussion of hacking these devices it would be remiss to not discuss the biggest vulnerability of all these devices. Each of these devices has the capability to be turned into a straight listening and/or recording device. Through tampering with the hardware or software it is possible to tell the device to constantly record and send the information elsewhere (e.g. a hacker or a government entity) while the device believes it is still communicating with the original destination. The tampering required to make these changes is not possible to perform remotely and strictly requires the physical changing of the device.

Technology companies such as Google, Amazon and Samsung have typically been responsive to discovered vulnerabilities of their devices but are not able to prohibit physical

changes made to their devices. A wikileaks document released details of a CIA project dubbed "Weeping Angel." This project allows the CIA to access Samsung SmartTV's via a flash drive and modify command execution and file transfer to put the microphone into a Fake-off mode where it appeared to be off but was still recording and transmitting data (Cullison, 2017). In this case since the breach was done manually through a flashdrive, it is extremely unlikely that Samsung would even be able to engineer protections against this sort of attack.

Companies have taken a stand to try and allow users to know when they are being recorded by having a LED light on the device that only lights up when the device is recording. Despite these steps at added protection, Amazon and Google have both filed patent applications for technology that would be increasingly probative into the lives of users. Both companies are working on the development of increased wake words so the companies can detect desires and interests to use for ad and product suggestions. This technology as Amazon calls it is a "voice sniffer algorithm" that adds another layer to the on-device voice analysis to pick up after hearing words like "love, bought or dislike" (Miller, 2018). Google, through their Nest Products, is working on the analysis of audio-visual signals to tell when a child is getting into mischief. It aims to analyze speech patterns and pitch to see if they match the profile of a child in the first place and sense whispers or silence indicative of mischief (Miller, 2018).

A Discussion of Devices - Other IoT

Voice activated devices are not the only smart devices contained within the home. The majority of devices within a smart home are actually not voice activated and rely on Bluetooth or Wi-Fi transmittance to an app or are consolidated by streaming through a voice activated app. These devices gather a constant stream of information on all characteristics of the house. Smart

devices in this category could include everything from small devices like a lightbulb or coffee maker, to large devices like a dishwasher or refrigerator, to even include the central thermostat or water meter. In this technological age every electronic item in a house can be integrated into a system to create a streamlined smart home. For this discussion of IoT in the home, two different types of data collection will be analyzed starting with the whole home system of Nest, and ending with a Samsung smart dishwasher.

Nest Products

Nest a company acquired by Google is one of the leaders of truly integrating the whole house into a smart home. They connect everything from utilities like AC and water, to door locks and outside security cameras (Nest, *Create a Connected Home)*. By connecting an entire home through a system like this, user's can control almost every aspect of their home remotely.

Due to the obscene amounts of information collected by these systems, everything sent over the Internet using Nest, is encrypted. Security experts found that due to this high level of encryption, Nest systems were almost impenetrable to attacks and were one of the safest systems on the market (Storm, 2014). The only way the system could be hacked was with penetration of the actual hub which required access to the physical device. Hackers found that by inserting a USB flahsdrive during boot up, they could write new programs onto the system and prevent data from being sent back to Nest (Storm, 2014). With no possible way for Nest to fix this loophole it could be both a point of vulnerability and potential for privacy. As the program does not interfere with the normal function of the product, users could install a program such as this to use the device without sending any data to Nest. Vulnerability however, lies in the fact that if the data is not being sent to Nest, it could be sent somewhere else. With data so pervasive it could tell a

hacker not only if someone is home, but what room they're in and their identifying demographics, the privacy concerns are obvious.

Even the privacy policy of Nest recognizes the gravity of the data collected and strives to have the strictest adherence to promoting users' privacy. For starters, they do not share personal information with third parties without explicit consent (Nest, 2018). They even make a point to not share personal information for commercial purposes (i.e. ads and marketing) without explicit consent which is a stark difference from Google. Steps have also been taken by Nest to make sure that transfers of data are protected. Multiple layers of protection and encryption such as HTTPS and Transport Layer Security protect data as it transfers between, the device, the users' phone and the cloud (Nest, *Frequently asked questions about privacy).*

The data collected is however used during the regular course of Nest's business. Data is used to help further develop and improve the products and services as well as make suggestions about usage to the user (Nest, 2018). Using the data in this way shows that while a user's data is protected from outside the company, it is subject to analysis and handling of employees within the company.

Samsung Smart Dishwasher

Hidden Touch Control Chef Collection Dishwasher with WaterWall Technology by Samsung is an example of what used to be a simple, household electronic that can now interact with its user, provide constant streams of data, and consequently, be regulated. Samsung smart appliances use standard encryption when transferring information between the appliance and the cloud (Samsung, *Privacy Policy).*

In terms of data usage, as noted above in the discussion of the Samsung SmartTV, Samsung collects and uses a large amount of data about their users. They use this data to customize messages like ads and promotional content. Data is also used for market analysis and to study the way people use the devices and services in order to improve them (Samsung, *Privacy Policy)*. Collected data is used by Samsung as part of the ordinary course of business and is aggregated to notice trends of usage. Samsung's privacy policy in general details many different third parties with whom they share consumer data. These entities include: affiliates, business partners, service providers, parties required by law, and parties in connection with corporate transactions (Samsung, *Privacy Policy)*.

Devices Within the Home

While the devices discussed above are only a small fraction of all possible smart devices within the home setting, they are a representative sample of the types of devices and the data they collect. Commonalities present across these devices are the use of encryption in the transfer of data between the device and the cloud storage. Encryption of this data provides an extra layer of privacy to users. If the data is encrypted during transfer and when stored on the device, users will feel more confident using the device and allowing the collection and transfer of their data. The ability to delete voice recordings from smart hubs also allows the user to have a higher sense of privacy. Regardless of false pickups by the device, enabling the user to control their data helps to add more privacy to the device's use.

Most companies also use the data to improve services for their customers. Since the smart hubs run on AI and are meant to learn from the data they collect, it is unclear which employees

or people actually handle the data. However, it is safe to say that the data collected is used in many aspects of the company. Departments from marketing to product development to finance in the company would likely use partial or whole data collected. Data collected would allow employees to figure out user stress points, fix any issues that the product is having, and find out how well their services are selling. Many of these companies will also share the data that is collected with third parties, creating an even wider net of people with access to users' data. Each company does inform the user of how they use their data through their privacy policies. However, these policies are often vague and completely ignored by consumers due to their dry language and length.

An unfixable hack about smart devices is the ability to physically hack them. While companies do a fairly good job at creating software and hardware that will stand up to malware and attacks from hackers, they are not impenetrable. Each of these devices can be subject to physical hacks usually coming from the breach of an infected flashdrive into a port on the device. Using this strategy, hackers were able to install software or rewrite certain functions of the devices that changed how they transferred information or recorded voice. Additionally, smart hubs can be tampered with beforehand to change these recordings and transmitting functions and still appear to be untampered with on the outside.

Fourth Amendment Applied

The Fourth Amendment refers to searches and seizures of "persons, houses, papers, and effects" and requires law enforcement to obtain a warrant based on probable cause to search or seize any of these things (U.S. Constitution). In analyzing data infringement under the Fourth

Amendment, it has to be broken down into two parts; first a determination of if a search occurred and then analyzed to see if a seizure occurred and what the invasiveness of the seizure was.

For a search to occur, it has to pertain to the physical property protected by the Fourth Amendment or the person must have a subjective and objective "reasonable expectation of privacy" on what is being searched. For primary purposes regarding data collection, there is no physical property, so searches under the Fourth Amendment of smart device data have to be analyzed under the *Katz* rule (*Katz v. United States,* 1967). Once it has been established that a search occurred, the lawfulness of the search comes into question. Under *Kyllo*, if the government is relying on technology not open to the general public, then that search would be considered unlawful under the Fourth Amendment (*Kyllo v. United States,* 2001).

If a lawful search has occurred, then the question of whether there was a lawful seizure must be analyzed. Under United States vs. Jacobsen, seizure was summarized as occurring "where there is some meaningful interference with an individual's possessory interests in that property" (*United States v. Jacobsen,* 1984). Meaningful interference is decided factually in a case by case basis, but can mainly be deduced as a restraint on a person's liberty by a person of authority. For a seizure to be reasonable, it is generally expected that the seizure provides a greater service to the public than it infringes on personal privacy. When considering the access of data from a third party, it is unclear where the search ends and the seizure begins particularly when the items in question are not tangible.

Under the third party doctrine, when a person voluntarily gives their information to a third party, they cannot have a reasonable expectation of privacy in regards to that data. On the side of the third party however, they can refuse to comply with a subpoena on the grounds that the information requested or "searched" is overly broad or that complying with this request

would place an undue burden on the company. The third party doctrine circumvents the person to whom the data pertains and focuses on the company holding the data to comply or refuse on behalf of their customer.

Legal Protections of the Smart Home

With full integration of the smart home and pervasive data being constantly collected on the intimate details inside a person's home, the opportunities for law enforcement to access this data are ever present and growing. However, as these opportunities are becoming increasingly more common, the law remains stagnant. As there are no real options to analyze the use of smart home data by law enforcement under appropriate law, it can only be analyzed under old precedent. To accurately look at the privacy loopholes covering this intimate data, this analysis will be broken into two parts; reasonable expectation of privacy and the third party doctrine with a privacy-oriented point of view.

Reasonable Expectation of Privacy of Smart Devices

Voice activated smart hubs, like Google Home and Amazon Alexa, rely on the transmittance of voice from the user to the device and back. In this sense, a conversation is clearly taking place between the device and the person. The user makes a verbal statement and waits for an auditory response back from the device. While in the usual sense a conversation takes place between two or more people, the exchanges people have with their smart hubs have the exact same external characteristics of a conversation with the verbal exchange of information between two parties.

Furthermore, a user's personification of their device helps cement these exchanges as conversations. People often talk to the voice assistants on their smart devices as if they are people. Alexa is commonly referred to with female pronouns "she" and "her",which personifies the technology. Additionally, users will ask their devices to "tell them a joke" or ask voice assistants personal information like they are a regular person. Integrated easter eggs into Alexa's software to respond with jokes or different stories to some requests show that even Amazon's programmers were expecting people to interact with their voice assistant as if it is a person (Stables, 2019). While this is a little more of a stretch with Google's voice assistant that is accessed by the pickup phrase "OK, Google" that does not as easily register as a person's name, the voice assistant also contains funny, easter egg responses that point to expected personable interactions with the device (Allison, 2018).

As people are expected to have a conversation with their voice assistant, false pickups would also be classified as snippets of conversation. For a false pickup to occur, there must be a person speaking within the pickup range. If the person speaking is talking to another person, then they are clearly having a conversation with that person. In the case that there is not another person present, then it is still construable that the voice snippet picked up as a result of an unintended pickup phrase could constitute a conversation, as the user has spoken to their voice assistant in the past in the same conversational manner that they would use with another person.

Under *White,* once a person confides in or shares information with another party, that information is no longer private. Voice recordings shared with a voice assistant could be analyzed as the speaker conversing with the voice assistant itself or in-fact the company whose database is going to provide the answer to the question through the voice assistant. Nonetheless,

once the information leaves the mouth of the user, it is no longer private and could be accessed at will by law enforcement.

From the earlier discussion on device security, it can be seen that the biggest universal vulnerability to smart devices is through physical penetration by a flashdrive. This requires physical intrusion of the property of a person. As physical property, intrusion would reasonably consist of search and seizure under the Fourth Amendment. The physical intrusion of the Jeep in *Jones* revealed that physical intrusion of an "effect" while under ownership of a citizen would constitute a search. If the intrusion occurred before the effect was owned by the party being searched as it did in *Knotts,* referenced by *Jones,* then the search and seizure was lawful (*United States v. Jones,* 2012). In other words, if the original owner, consents to the altering of the item and the party being searched accepts the altered item regardless of their knowledge of the alteration, the subsequent search and seizure is lawful.

This goes to say that if a law enforcement agent wished to alter a smart device and have a unrelated party give the device to the party they intend to search, this is lawful under *Jones*. Smart hubs which can be turned into listening devices quite easily could provide the ability for law enforcement to legally listen to all conversations inside of a house due to this loophole.

Kyllo however provides a competing conclusion to usage of smart device data. Under *Kyllo,* the government is prohibited from using devices not in public use to gain intimate details of the house that would otherwise require physical intrusion. All smart devices do not publish their data to the general public and in fact go through great lengths to keep this data private. Due to the nature of these devices, with their ability to collect an exorbitant amount of intimate data easily and their equal attempts to protect it, conclusions from *Kyllo* would argue that the use of these devices and their data would be unlawful under the Fourth Amendment without a warrant.

Overall the "reasonable expectation of privacy" test has two prongs, those being that the person has exhibited an expectation of privacy and that society would recognize that privacy as reasonable (*Katz v. United States,* 1967). In *Smith,* it was decided that although people had no reasonable expectation of privacy over the numbers they dial, they do have an expectation of privacy over the content of their calls (*Smith v. Maryland,* 1979). Even though the call still goes through the phone company and is transmitted as part of their business, the Court still held that people had a reasonable expectation to the privacy of the content of their call. In the same way, the voice recordings by smart hubs should be protected in content. In both situations, information via voice is being transferred from one party to another.

The expectation of privacy that people exhibit in the use of their smart devices in their homes is apparent in their usage. Devices like Nest that aim to truly link up all aspects of a home under one system can amass a frightening amount of information about the house and the people in it at any given time. For example, a Nest system can be used to lock the doors of the house which, along with external and interior cameras, would allow the system to know whether or not there is anyone within the home. The cameras and voice recognition software are also working on being able to tell who the person is and in what room they are. Privacy is not only expected but demanded for users to put confidence into a system that is able to gather such intimate data.

Not only is the expectation of privacy in the use of these devices subjective, but it is objective as well. With the use of heavy encryption to transfer data from the device to the cloud, it is clear that companies have taken intensive measures to ensure their customers feel safe using their product. Companies also make a point to host hackathons to invite people to attempt to hack into their devices and use the results to make their devices more secure. The privacy

expected in the use of these devices is not just subjective but has been validated by the companies and the public at large.

Although the data collected is highly personal and private, it all would still fall under the current extrapolation of the third party doctrine developed in *Smith* and *Miller*. Under this doctrine, if information is voluntarily given to a third party, the original person cannot have a reasonable expectation of privacy of this data. In this technological age, it should come to no surprise that companies are collecting and using the data recorded by these smart devices. Nevertheless, the average consumer does not read a product's privacy policy or terms of use and clicks the "accept" button or buys the product and has their consent implied with very little knowledge about how the device works.

Therefore, the question of "voluntary" comes into issue. If a person does not have a full understanding of how a product works, it is hard to say that they are voluntarily giving their consent to the collection and use of their data by a third party. In *Carpenter*, the Court noted that "there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers," and that "cell phone location information is not truly 'shared' as the term is normally understood" because "a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up" (*Carpenter v. United States,* 2018).

The same reasoning when applied to smart devices still holds. Smart devices within the home are constantly and effortlessly collecting information about the current state of the home. These devices automatically collect data as part of their operation whether it be voice recordings or thermostat temperatures. Smart devices which work by using AI to improve their function and

IoT to communicate with other devices must collect and store a constant stream of data to work. However, these devices do not ask the user each time they record a data point, which would be the only way the collection of data would be truly voluntary.

The holding in *Carpenter* denied to extend the third party doctrine to cell site data in part due to level of intrusiveness and extensiveness of the data collected (*Carpenter v. United States,* 2018). By any definition, the data collected by smart devices which constantly measures "vitals" throughout the home, is overly intrusive and extensive. In reference to *Kyllo,* where a home is considered "*all* details are intimate details," and smart devices are constantly collecting these details (*Kyllo v. United States,* 2001).

There have been recent signs of evolution in the Court and a desire to better protect citizens' private data. The Court in *Riley* showed evolution in privacy rights by placing phones in their own category due to the amount of personal data they contain (*Riley v. California,* 2014). While this case was decided in 2014 and technology has evolved at an extreme rate since then, the Court seems to be acknowledging that current privacy laws are not keeping up with the rate of technological development.

At this point in time, it is hard to say for sure where the Court and legislature will go in regards to personal privacy in a technological world. Due to the highly intimate and extensive nature of the data, it is clear that to keep citizens' privacy rights at the forefront, law enforcement officers must be required to obtain a warrant before accessing this personal data. While this may slow down the process of "catching bad guys," the Fourth Amendment is meant to make citizens feel secure in their own homes. Without requiring law enforcement to obtain a warrant before using smart device data, they could conceivably at will tap into a person's living room Nest Camera, eavesdrop through their smart hub, or tell if anyone is home from their smart door lock.

This in some ways is an Orwellian view of law enforcement but remains a very real possibility at this point in time without any clear guidance on how these issues will be addressed in a court of law.

Issues and Objections

Issues pertaining to this topic mostly consisted of outdated governing rules. As the legislature has to enact a new law or the Court has to hear a case on IoT to truly have any governance over IoT and the Fourth Amendment, all cases pertinent to the subject are seemingly outdated in their approach to the topic.

Fourth Amendment

Strict interpretation versus adapted interpretation of the Constitution remains a big rift in the Supreme Court. Some are on the side of interpreting in direct accordance with what the justices believe to be the intended purpose of the Amendment, and yet others side with recognizing the limitations of the Constitution and adopting it to remain relevant. While there remains no clear answer on this topic, it is of great importance to how the use of IoT within the home will be governed.

Justices on the side of strict interpretation use the Fourth Amendment to mean that the Constitution was intended to provide thorough protection from the government particularly in the "constitutionally protected areas." On the other side, justices who favor adapting the constitution to the present are in favor of a reasonable expectation of privacy viewpoint. It is unclear which side the Court will lean towards when this issue comes before it or if there will be additional

relevant legislation. Regardless, the constitutional interpretation of the Court will be extremely important in ultimately deciding the privacy rights of citizens in relation to the smart home.

Third Party Doctrine

The third party doctrine is even more unfit to deal with the age of cloud computing than the Fourth Amendment. With an increasing number of Americans using the cloud to store their files, the third party doctrine seems to be ridiculously overbearing. It is no longer uncommon for people to have all of their pictures stored on the cloud via Google Photos or Apple's iCloud. People also use services like Dropbox and OneDrive to store all of their personal and work files. The use of the cloud opens up a massive amount of files to be subject to government snooping through the third party doctrine.

In issues of electronic data, the lack of notice of seizure becomes important. Prior to computers, for government officials to seize something, they had to give notice of the seizure. With electronic data, especially when it is stored through a third party on the cloud and can be subpoenaed from the company instead of the person, there is no notice. A person could have their private electronic records searched and seized by government official while being completely unaware it was happening.

Riley vs. California

In *Riley*, the Court brought up a fascinating point that could be pivotal to the evolution of cloud based law. They noted that the information being searched was on the cloud and therefore not truly on the person being searched. Classifying cloud based data as not being on the device

on which it is recorded, in this case a cell phone, could open the door to a lack of Fourth Amendment protection on smart device data collected in the home.

For the Court to recognize that the data accessed through smart devices is not on the device questions if data collected from smart devices in a home is within the home. If the data is not on the device then it would not be protected under the Fourth Amendment. While there should be a distinction between data accessed through a smart device and data collected by a smart device, it is hard to say that the Court will make this distinction when the time comes. This could potentially bring *Kyllo* back into the limelight by using the test of physical intrusion (ie could the government know this information without physically being inside the house) instead of *Katz* "reasonable expectation of privacy" test.

References

18 U.S. Code § 2703. (d)

Allison, C. (2018, December 06). The 70 best Google Home Easter eggs to try right now. Retrieved from https://www.the-ambient.com/features/best-google-home-easter-eggs-166

Amazon. *Alexa Terms of Use.* Retrieved from https://www.amazon.com/gp/help/customer/display.html?nodeId=201809740

Amazon. *Requirements for Cloud-Based Wake Word Verification.* Retrieved from https://developer.amazon.com/docs/alexa-voice-service/streaming-requirements-for-cloud-based-wake-word-verification.html

Amazon. *Review Your Voice Recordings.* Retrieved from https://www.amazon.com/gp/help/customer/display.html?nodeId=201602040

Bursky, D. (2011, July 08). Secure Microcontrollers Keep Data Safe. Retrieved from https://www.digikey.com/en/articles/techzone/2011/jul/secure-microcontrollers-keep-data-safe

California v. Greenwood, 486 U.S. 35 (1988)

Carpenter v. United States, 585 U.S. ___ (2018)

Chimel v. California, 395 U.S. 752 (1969)

Chokshi, N. (2018, May 25). Is Alexa Listening? Amazon Echo Sent Out Recording of Couple's Conversation. Retrieved from https://www.nytimes.com/2018/05/25/business/amazon-alexa-conversation-shared-echo.html

Cullison, A. (2017, March 8). WikiLeaks Reveals CIA Hacking Projects, From Weeping Angel to Hammer Drill. Retrieved from https://www.wsj.com/articles/wikileaks-reveals-cia-hacking-projects-from-weeping-angel-to-hammer-drill-1489017814

Google. Data security & privacy on Google Home. Retrieved from https://support.google.com/googlehome/answer/7072285?hl=en

Google. *Privacy Policy.* Retrieved from https://policies.google.com/privacy

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

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

Miller, A. (2018, April 3). Amazon patent reveals 'voice sniffer algorithm' that could analyze conversations. Retrieved from https://abcnews.go.com/Business/amazon-patent-reveals-voice-sniffer-algorithm-analyze-conversations/story?id=54175793

Montag, A. (2018, September 04). Former NSA privacy expert: Here's how likely it is that your Amazon Echo will be hacked . Retrieved from https://www.cnbc.com/2018/09/04/ex-nsa-privacy-expert-how-likely-your-amazon-echo-is-to-be-hacked.html

Nest. *Create a Connected Home*. Retrieved from https://nest.com/

Nest. *Frequently asked questions about privacy.* Retrieved from https://nest.com/privacy-faq/

Nest. (2018). *Privacy Statement for Nest Products and Services.* Retrieved from https://nest.com/legal/privacy-statement-for-nest-products-and-services/

Pursche, O. (2017, February 24). Testing Amazon Echo Dot & Alexa App. Retrieved from https://www.iot-tests.org/2017/02/testing-amazon-echo-dot-alexa-app/

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

Samsung. *Privacy Policy.* Retrieved from https://www.samsung.com/us/account/privacy-policy/

Samsung. *Samsung Privacy Policy -- SmartTV Supplement*. Retrieved from https://www.samsung.com/sg/info/privacy/smarttv/

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

Stables, J. (2019, March 09). 123 brilliant Alexa Easter eggs: Funny things to ask your Amazon Echo. Retrieved from https://www.the-ambient.com/guides/best-alexa-easter-eggs-167

Storm, D. (2014, August 11). Black Hat: Nest thermostat turned into a smart spy in 15 seconds. Retrieved from https://www.computerworld.com/article/2476599/black-hat-nest-thermostat-turned-into-a-smart-spy-in-15-seconds.html

U.S. Constitution, Amendment 4

United States v. Jacobsen, 466 U.S. 109 (1984)

United States v. Jones, 565 U.S. 400 (2012)

United States v. Kirschenblatt, 16 F.2d 202 (2d Cir. 1926)

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

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

United States v. Robinson, 414 U.S. 218 (1973)

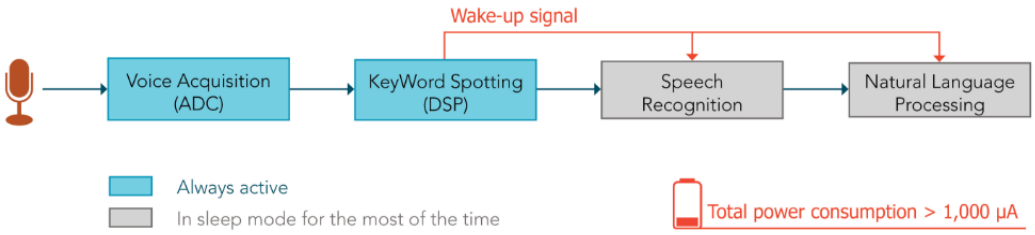
United States v. White, 401 U.S. 745 (1971)

Wang, A. B. (2017, March 09). Police land Amazon Echo data in quest to solve murder. Retrieved from https://www.chicagotribune.com/bluesky/technology/ct-amazon-echo-murder-wp-bsi-20170309-story.html

Zhang, Y., Suda, N., Lai, L., & Chandra, V. (2018, February 14). Hello Edge: Keyword Spotting on Microcontrollers. Retrieved from https://arxiv.org/abs/1711.07128

Appendix

Chart 1: Diagram of KeyWord Spotting



Some Technical Aspects - Timeline

1970s: DES was the result of a research project set up by International Business Machines (IBM) corporation in the late 1960's which resulted in a cipher known as LUCIFER. Lucifer that had a key length of 128 bits. The key was later shortened to 56 bits and renamed DES (technical advise from government agencies were received). The U.S. government officially adopted DES.

1991: Philip R. Zimmermann is the creator of Pretty Good Privacy (PGP). For that, he was the target of a three-year criminal investigation because the government held that US export restrictions for cryptographic software were violated when PGP spread all around the world following its 1991 publication as freeware. After releasing PGP as shareware, someone else put it on the Internet and foreign citizens downloaded it. Cryptography programs in the United States are classified as munitions under federal law and may not be exported. The US government dropped the case in early 1996. The Zimmermann case is the story of an innocent person fighting for his rights against the abuses of big government

2007-?: PRISM is a code name for a program under which the United States National Security Agency (NSA) collects Internet communications from various US Internet companies (Microsoft, Apple, Yahoo, Google, Skype). The US National Security Agency and Federal Bureau of Investigation have been harvesting data such as audio, video, photographs, emails, and documents from the internal servers of nine major technology companies, according to a leaked 41-slide security presentation obtained by The Washington Post and The Guardian…

2019: wikileaks

Technical Challenges IoT

The recently-published article " Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-scale IoT Exploitations" shows that many vulnerabilities are preventable. Causes include:

- Inadequate authentication
- Improper encryption
- Unnecessary open ports
- Weak programming practices (e.g. root user, lack of SSL, plain text password, backdoor, etc.)

Recent attacks

- IoT toys leaking millions of voice messages (2016)
- Baby monitor "converses" to children (2015)