5-18-2019

Privacy in the 21st Century: DNA and the Fourth Amendment

Julia Clements

Privacy in the 21st Century

DNA and the Fourth Amendment

Julia Clements

Senior Honors Thesis

Messiah College

May 2019

Introduction

Imagine you are sitting at your home watching a television program with your family one average weekend night. Suddenly, you hear a sharp knock and the doorbell rings. When you open the door, you discover several uniformed police officers waiting to take you away. The officers explain that you are a suspect of a serious crime based on DNA you never gave voluntarily. They found you through your third cousin's profile on an online genetic database. Using his genetic information, they were able to match the familial line to a sample from the crime scene and use known information to determine you are the suspect. You begin to wonder how this could be legal and whether or not your privacy been infringed.

The issue of privacy has always been a serious concern, only becoming more prominent in the political sphere as technology advances and police investigations seek new ways to solve cold cases. In the law enforcement realm, there is a very fine line between investigating and taking away someone's privacy. It is crucial that police stay on the investigative side of the line or else they face consequences such as testimony or evidence being inadmissible in court.

One of the main rules that police and other law enforcement professionals must follow is the Fourth Amendment of the United States Constitution. It 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 person or things to be seized" (Bill of Rights). Essentially, the police must have some sort of proof that the item they are looking for is likely to be in the place they wish to look. In order to search that location legally, the officers must go before a judge and present their reasoning in order to obtain a search warrant.

Privacy has become a major issue with regard to the Fourth Amendment because of the fact that law enforcement must invade an individual's personal life in order to solve many cases. They often are required to search a person's home or workplace and look through sensitive information to find proof of a crime. The Supreme Court has ruled many times on various aspects of privacy and police procedure to define the parameters of a legal search and seizure. These cases have dealt with everything from wiretapping a public phone booth to triangulating a cell phone's location during an investigation.

The issue of DNA comes into play when one considers the fact that it is not possible to get a blood or hair sample from the accused without them knowing. A warrant is needed but the police must be able to show that there is probable cause that the individual is the culprit. Technological advances within the digital realm have created a grey area with regard to an individual's privacy. On several occasions, police have used online genetic databases to find the perpetrator, usually without a warrant. This creates an issue because no one knows exactly where the privacy line is or how far officers can legally go.

Ultimately, there are two major questions that must be answered. How has the usage of DNA in the criminal justice field impacted the United States' understanding of the Fourth Amendment? How has DNA altered the privacy rights of Americans throughout its use in criminal procedure? Due to decisions in a variety of Supreme Court cases, Americans are entitled to privacy in areas where they should have a reasonable expectation of it, whether it is their homes or stepping away from a restaurant table to have a private conversation. DNA is a much newer addition to criminal procedure and privacy. Within the past few decades, DNA has become a major part of criminal investigation. For the most part, unless an individual is a

suspect in an investigation or the police have a legitimate reason to need their DNA, that individual's DNA cannot be taken.

As long as law enforcement officers follow the proper procedures and abide by relevant case law, they are allowed to search and infringe on an individual's privacy, within reason. However, even in newer areas that do not yet have an abundance of case law and regulations, police should still be required to follow the same procedure. It is crucial that an individual's privacy is not unnecessarily invaded, so on newer issues such as digital genetics, police must be held to the same high standard they already follow.

It is first essential to look at a brief history of DNA's usage in the courtroom and a few of the current accepted techniques. Next, a step back in history to explore why privacy issues became so prominent in American society will be discussed before moving on to several Supreme Court cases that deal with privacy and technology. Finally, several propositions for the best way to deal with genetic privacy in the future will be discussed before progressing to the direction the Supreme Court should take with regard to law enforcement's treatment of both physical and digital DNA.

What is DNA Profiling?

The overarching technique for DNA analysis is known as DNA profiling. As the name suggests, DNA profiling is where criminal investigation joins science. Although it might seem obvious, DNA profiling can only be used as in an investigation where DNA is found at a crime scene. One issue of DNA profiling in current society is known as the CSI Effect; due to the popularity of crime shows that for the most part inaccurately depict how real investigations work, most people on juries expect DNA evidence. This complicates things because it is not

always found at crimes such as arson. In cold cases that are later solved, DNA evidence is not always available because investigators did not necessarily know to collect it.

DNA profiling allows investigators to determine whether or not someone was at the scene of the crime and is the likely culprit. Previously, only things like blood typing were available; however, the issue with this is that there are only a few types of blood. This could really only be used to determine that a person was innocent and narrow down a suspect pool (Easteal, McLeod, and Reed 4-5). Fortunately, since everyone has a unique set of DNA, this technique can be used conclusively to help determine guilt.

One common type of DNA profiling is known as gel electrophoresis. In order to do DNA profiling, the scientist first needs to apply a special restriction enzyme that marks specific sets of DNA that will be looked for in samples. The DNA samples are then placed into a special gel which is inserted into a machine. The machine applies an electric current that causes DNA to pass through the gel; smaller fragments move farther than larger ones (Easteal, McLeod, and Reed 47). In order to determine if any of the samples match the crime scene samples, the movement patterns are analyzed; they generally occur as several bands within the gel. The spacing between bands is measured and a match occurs when the band spacing is identical (Ibid 88).

The Origins of DNA in Crime Investigations

In 1983, in the town of Leicestershire, England, a fifteen year old girl, Lydia Mann, was found raped and murdered in a secluded area. Unfortunately, three years later, all leads had turned into dead ends, so the case went cold. However, in 1986, another girl, Dawn Ashworth, was found in similar circumstances to Mann in a nearby village (Aronson 15). A local teenage

worker confessed to the crime so police asked Dr. Alec Jeffreys to test samples using his DNA profiling technique; it had successfully been used in many immigration cases and had gained legal legitimacy in court. Although Jeffreys was able to determine that the same person had committed both crimes, the worker's DNA was not a match (Ibid). As a last effort to find the murderer, police decided that all young men in the vicinity of the crimes should be subject to voluntary blood and saliva samples. After the samples of over 4,500 men were analyzed, there was still no match. The police finally received a break when they got a tip to investigate a man named Colin Pitchfork. He had convinced a coworker to give a sample while pretending to be him. Once Pitchfork's sample was gathered, analysis showed his DNA was, in fact, a match for the murderer of both girls. Six years later, a case was solved due to the introduction of a new analysis technique (Ibid 17).

This case, in a small, quiet village of England, caused a revolutionary change in crime scene investigations. DNA profiling quickly became accepted and widely used. Now, instead of relying only on evidence that could be seen by the naked eye, investigators could start to collect other sorts of evidence that could be scientifically analyzed at a forensics lab. Proving guilt would be much easier because a genetic match is harder to dispute than something like an eyewitness testimony.

After gaining popularity in the United Kingdom, DNA profiling clearly did not stay confined to that country. In 1987, the first case in the United States was solved using DNA. Police in Orlando had discovered similar characteristics in a number of rape cases that led them to believe they were dealing with a serial rapist. The individual went to great lengths to ensure that very little evidence, if any, was left behind (Aronson 33). The first of the man's victims, Nancy Hodge, was able to pick the suspect out of a lineup. Although prosecutors had the

positive identification, they needed something more conclusive; blood typing and fingerprinting provided circumstantial evidence but nothing that actually proved who did it. Realizing that DNA was a rapidly developing field, prosecutors decided to try it. They obtained a sample from their suspect, Tommie Lee Andrews, and received a positive match (Ibid).

In order for the evidence to be admissible in court, prosecutors just had to have a witness testify that DNA was a reliable source of evidence. They were easily able to do this as DNA had become a standard scientific practice. Their witness, Dr. David Housmann, testified to its reliability and pointed out that the probability of a coincidental match was one in ten billion (Ibid 38). Like the British case, DNA's admissibility was rapidly expanding. Investigators were quickly finding new ways to determine guilt.

Early Challenges to DNA

Despite rapid acceptance of DNA as an investigation technique, it is crucial to acknowledge some of the challenges it faced throughout its journey to approval. The first revolves around the fact that everyone was so eager to push for the acceptance of DNA profiling that they forgot to look at its limitations and downfalls. In order to gain legitimacy, lawyers were bringing in scientists who did not specialize in the area of forensics. One serious concern was that when looking at samples for immigration disputes or other voluntarily offered samples, analysts have access to as much DNA as they need in order to run several tests. However, at a crime scene, there may only be a minimal amount of DNA that can be obtained from a small blood smear; this could mean that only one test can be run (Aronson 59). While the prosecutors were bringing in experts, they were not as knowledgeable about forensic DNA as they should have been. This is not to say that DNA has not been an incredibly useful addition to the criminal

justice field. It just would have been more helpful to accept only those techniques that were actually useful and provided reliable answers. Only a short time after accepting DNA's admissibility, several techniques had already been found that were not acceptable; many of them had been used to convict a large number of innocent people (Ibid 58).

Another major issue to be acknowledged was the fact that in a few instances, labs were taking DNA results that should have declared an individual innocent and altering them so the person would be seen as guilty. In 1998, a high school student, Josiah Sutton, was arrested and convicted for the rape of a woman. A forensics lab found that Sutton's DNA matched that of one of the woman's rapists; a lab scientist even testified to the accuracy of the tests. However, just four years later, Sutton was released after it was discovered that the lab had twisted his test results to get the conviction (Aronson 203). Sutton's case, along with several others, led an audit of DNA procedures to conclude that, "crime labs cannot police themselves…" (Ibid 205). This provides a crucial warning that mistakes can be extremely detrimental to someone's life. It is never acceptable to allow the desires of one to harm the life of another. In this circumstance, a boy lost out on four years of his life because of a lab worker.

21st Century DNA Developments

In 2004, the voters of California approved Proposition 69, which required that DNA be collected from all felons, as well as any adult or child arrested for certain severe crimes. This DNA then needed to be uploaded to the state DNA database. This was crucial, because it could allow police to connect crimes based on similar DNA evidence, or to connect individuals to previously unsolved crimes. It also could potentially also allow more crimes to be solved if they crossed county or jurisdictional lines (Proposition 69). Privacy concerns for anyone ultimately

found to not have committed the crime are also addressed. If one had to give a DNA sample as part of the investigation, once police determine the individual is no longer a suspect, that individual can request that their sample be removed from the database. Proposition 69 also provided basic guidelines for having DNA removed from the database if one was convicted of a crime. Essentially, if the person was not convicted of a felony or was convicted of a misdemeanor with no prior felony record, they were allowed to apply for removal (Proposition 69).

A second major development in DNA does not have to do with legislation or keeping the police in check; it deals instead with a new application of DNA profiling. Instead of using a direct DNA sample, such as blood or saliva, analysts have developed a technique known as DNA familial profiling. In essence, an investigator takes DNA found at a crime scene and tries to match it with DNA in a database. A partial match shows that there might be a familial relation between the individual in the database and the individual whose DNA appeared at the crime scene (Roewer). Once a match has been found, police then must use more traditional investigative techniques to locate potential relatives of the individual who could match the DNA or profile from the crime scene.

The first instance of this occurring was to convict a British man of murder in 2004. Michael Little was killed when he was hit by a brick thrown by a drunken person. Several attempts failed to find the culprit by looking in DNA databases for a match to the blood spot found on the brick. As a last effort to find the killer, investigators looked in the databases again; this time, they decided to accept partial matches. They narrowed the possible matches down from a few thousand to only twenty-five. One of the individuals found in the database had a brother, Craig Harman, who soon admitted to the murder (Krimsky & Simoncelli 64). This

desperate search for an answer ended up creating a new technique and revolutionizing how DNA databases could be used for finding suspects in cold cases.

One very recent, famous case of DNA familial profiling involved the Golden State Killer. From the 1970s-80s, someone was committing a large series of crimes throughout California. Several characteristics were the same across all crimes, so law enforcement was able to determine that the crimes were committed by the same person; DNA analysis helped to confirm this theory. Dozens of rapes, murders, and break-ins were all attributed to this individual. However, the case eventually went cold as all attempts to catch the perpetrator were unsuccessful (Lussenhop). Due to the rise of online public genetic databases, someone was able to match a relative's DNA with samples from the crime scenes. Finally, several decades after the first crime, Joseph James DeAngelo, a former police officer, was arrested and charged with this crimes.

Issues with DNA and Privacy

On the surface, there seems to be nothing wrong with using public DNA databases to track down criminals. However, several concerns are brought to light when this investigative technique is analyzed from the standpoint of privacy. The database used to catch the Golden State Killer, GEDmatch, is a database where individuals can upload their genetic profile in order to research their ancestry. Users are informed that their DNA could be used for things other than just genealogy. That being said, the creator of the site was not aware that law enforcement officials used his site to find a perpetrator until after it had been made public (Brown). If the creator was not aware, then the individuals who used his site certainly were not aware.

UC Berkeley professor Andrea Roth addresses one of the major privacy concerns with this technique. As she explains, "When you put your information into a database…and law enforcement has access to it, you may be unwittingly exposing your relatives…to scrutiny by law enforcement. Even though they may have done nothing wrong" (Brown). Although this technique helps law enforcement to solve cases, it allows them access to the private information of innocent people. Normally, this would not be the case. Police would have to show probable cause in order to conduct a search. However, in this instance, it almost appears as if they were just trying something to see if it would produce any results. This is dangerous because it infringes on the freedom of innocent individuals. Although the website states that the DNA can be used for any number of things, the average person likely would not think of a criminal investigation application when deciding whether or not to upload his or her DNA profile. Roth also states that, "If we allow the government to use [DNA familial profiling] with no accountability or no further safeguards, then all of our genetic information might be at risk for being used for things we don't want it to be used for" (Brown). If no restrictions are placed on law enforcement access to online genetic information, then theoretically this opens the door for all kinds of unregulated investigation as long as police can connect it in a vague way to a case. Before going on to look at what should happen in the future, a historical lens is a second essential way to view this subject.

The Problem of Privacy Law

In the 1960s, there was a major debate among legal scholars because they could not decide whether or not a right to privacy was a reasonable right for Americans to have. One group, called the conceptualists, insisted that rights could only come from actual laws, whether

codified or common. The other group, realists, wanted to look at privacy rights from the context of experience and societal values (Hasian Jr 91-94). Unable to compromise or find any common ground, the two groups turned to the work of Samuel Warren and Louis Brandeis to come to a conclusion. Warren and Brandeis had located a concrete legal precedent in countless legal cases, as well as appearing to have a devotion to social issues and the values of the time (Ibid).

During this same era, there was also a rising desire for privacy in the public sphere. Documents and reports were emerging, telling the American public that government actions such as surveillance had gone too far. They were intruding into the private lives of citizens without apparent cause (Hasian Jr 97). A report published in 1976 by the Senate Select Committee to Study Government Operations with respect to Intelligence Activities, details many of these infractions. Thousands of FBI files were opened on innocent members of potentially threatening organizations (they were in no way threats), to be used if they ever applied for a federal job. In addition, countless American citizens were illegally wiretapped, bugged, and surveilled without the proper warrant ("Senate Committee" 280-283).

Several terms used during this time help to explain the discontent of American people. "The octopus" and "snooper state" were two of the more common phrases to infiltrate American conversation. The media ultimately helped play a role into the push for privacy, by using these terms and beginning to associate them with anyone violating privacy. As a "snooper", the government was trying every way it could to infringe on privacy; some even claimed they were using census takers. As an "octopus," the government was allowing "tentacles of its creepers [to] pierce the walls of all the homes in the land" (Hasian Jr 99-100). Paranoia in American society made it impossible to do even the simplest of tasks, such as taking a trip to the local shopping mall, without fear that prying eyes were watching. With this intense apprehension, it

only made sense that the judicial system would need to step in at some point. This occurred when the Supreme Court heard *Griswold v Connecticut* in 1965.

Griswold v Connecticut

Griswold v Connecticut, which took place in 1965, was one of the first Supreme Court cases to acknowledge an overarching idea of privacy rights. It had to do with an 1879 Connecticut law that banned contraceptives under any circumstances. Griswold, who was associated with Planned Parenthood, was involved in the opening of a birth control clinic; the clinic gave contraceptive advice to a married couple before being shut down (*Griswold v Connecticut* 480). The clinic was created solely for the purpose of attempting to argue that the Connecticut law was unconstitutional (Ibid).

In a 7-2 decision, the Supreme Court ruled that the law was indeed unconstitutional. Both the majority decision, written by Justice Douglas, and the concurring opinions were rooted in various aspects of the Bill of Rights and the Fourteenth Amendment. Douglas wrote that aspects of the Bill of Rights created "zones of privacy". The very text of the Fourth Amendment creates privacy. The police cannot just demand to walk into a person's residence and search; they must have probable cause, so that they do not infringe on an individual's privacy (*Griswold v Connecticut* 484). Although privacy was not explicitly stated in the Constitution, the Court is clearly stating that it is a right. In order to act and live one's life freely, they need to be secure in the knowledge that they will not be punished for their actions.

Defining Privacy in an Investigative Context

The first major case that dealt specifically with privacy and the Fourth Amendment was *Olmstead v US*, decided in 1927. The circumstances of the case revolve around the constitutionality of wiretapping. Olmstead was suspected of breaking the National Prohibition Act by transporting and selling alcohol. In order to determine the validity of their suspicion, federal officials wiretapped phone lines to Olmstead's office. Officials were able to confirm that the Act was being broken (*Olmstead v US* 438).

In the majority opinion, Chief Justice Taft wrote that the wiretapping was constitutional under the Fourth Amendment. In this case, the Court took a fairly literal interpretation of the Amendment, saying that something physical needed to happen in order for a search or seizure to occur. This decision created the physical trespass rule. In order for a search to occur, there needed to be some sort of physical location to be entered or tangible item to be seized. The conversations between Olmstead and his associates were not tangible items. Therefore, no search occurred; the Fourth Amendment was not in question here (*Olmstead v US* 451). The conversations were completely voluntary and not coerced whatsoever. Taft wrote that "The language of the Amendment cannot be extended and expanded to include telephone wires reaching to the whole world from the defendant's house or office" (Ibid 465).

In his dissent, Justice Brandeis compares mail tampering to wiretapping. He states that mail tampering is much worse, but that the two activities are essentially the same; they are both public services carried out by the government. He quotes Federal Judge Rudkin who said, "True the one is visible, the other invisible; the one is tangible, the other intangible; the one is sealed and the other unsealed, but these are distinctions without a difference" (*Olmstead v US* 475). Essentially, whether or not the evidence obtained was physical, it should not matter. Due to the

fact that the citizen was having a personal conversation in an area not freely accessed by the public, the government would be trespassing on a private area, even if its agents did not physically enter it. This case shows that the Supreme Court was willing to look specifically at privacy with regard to the Fourth Amendment. They were willing to consider that explicit regulations on the power of law enforcement professionals needed to be made.

Although the decision in *Olmstead* was revolutionary in terms of the concepts it discussed, the actual decision itself was short-lived. It was overturned only forty years later, in 1967, by *Katz v United States*. The case again dealt with the issue of wiretapping but in slightly different circumstances; it looked at semi-public places instead of private locations. Katz was suspected of using a public phone booth to pass illegal gambling wages across state lines. In order to test this theory, federal agents bugged the outside of the phone booth. Due to this evidence, Katz was arrested and his conviction was upheld by the Court of Appeals (*Katz v US* 347).

Fortunately for Katz, the United States Supreme Court took a drastically different opinion as to the constitutionality of this investigation. In a 7-1 decision, Justice Stewart delivered the majority opinion which offered an alternative to the "physical trespass" rule that had been established by *Olmstead*. One notable line from his opinion states that "the Fourth Amendment protects people, not places" (*Katz v US* 351). If the Amendment were intended to protect places, there would be no mention of people in its text. By deciding to enter a public phone booth, Katz was looking to have a private conversation away from others, or as Stewart puts it, he was looking to avoid the "uninvited ear" (Ibid 352). In a concurring opinion, Justice Harlan established the reasonable expectation of privacy rule, as it came to be known. He states that there are two requirements for privacy to be reasonable. It must be somewhere a person could

have an "actual expectation of privacy" and society must be willing to view that expectation as reasonable. He goes on to describe a public phone booth as "a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized by reasonable" (*Katz v US* 361).

The sole dissenter, Justice Black, argued that his majority counterparts are misunderstanding the words of the Fourth Amendment. Both clauses, the explanation of the protected entities as well as the requirements for a warrant, describe tangible entities; according to him, the spoken word is not a tangible item. Black agrees with the rationale provided by the Court in *Olmstead v US*, because it looks at what the Founding Fathers wanted when they wrote the Amendment. When the Fourth Amendment was written, eavesdropping was a common practice; if the Fathers had wanted to restrict it, they would have done so explicitly (*Katz v US* 366). Black does not believe that it should be interpreted so as to bring it up to modern times (*Katz v US* 365-6). Despite this rationale, Black's argument is flawed, as the telephone would not be invented for about 100 years after the Constitution was ratified. Therefore, the Founding Fathers' main forms of communication would be letters and physical conversations. They had no way to account for the telephone and the major role it would ultimately play in society and the potential that issues regarding privacy would come up. In addition, the average American likely would not appreciate discovering that communications they believed were private were actually being surveilled, so it seems unreasonable to allow the continuing of the unsavory practice.

This case drastically changed the way the judicial system looked at privacy. Instead of only needing to worry about physical trespass being a violation of privacy, law enforcement now needed to be aware of new rules. They had to ensure that their investigation did not infringe on a reasonable right to privacy.

Privacy at Home

Several times, the Supreme Court has been asked to examine one's expectation of privacy within his home. In 2001, an intriguing case, *Kyllo v US*, looked at whether or not a thermal imaging device could be used without a warrant. Upon suspicion that the defendant, Danny Kyllo, was growing marijuana in his home, an officer used a thermal imaging device to see how much heat was coming from inside the home; this was done without a warrant. It was discovered that the heat signature was consistent with growing marijuana plants and this evidence was used to obtain a warrant to search the inside of the home (*Kyllo v US* 28).

In the Court's majority opinion, Justice Scalia writes that this practice is unconstitutional because violates the Fourth Amendment. He states that at the very core of the Amendment is the idea of being able to expect privacy within one's home (*Kyllo v US* 31). Had the officer only been observing the home's exterior, this case would be entirely different. However, according to the majority, the heat signature was only found through the invasion of the interior (Ibid 33-34). Scalia goes on to refute the government's belief that privacy concerns are not relevant here because no personal information was gathered. He argues that throughout American history, "the Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained" (*Kyllo v US* 37). A practice is either allowed or it isn't from the very start; there is no principle of waiting to see if the gathered information meets an arbitrary guideline.

Privacy and the Street Curb

California v Greenwood, a 1988 case, deals with the seemingly bizarre topic of filled trash bags but adds an important point to the questions of American privacy and acceptable law

enforcement practices. After getting several reports of suspicious activity, such as vehicles going to Greenwood's home at unusual times of the night and only staying for a minute or two, local police requested and obtained the trash bags from in front of the home. After searching through the trash, a warrant was issued based upon drug paraphernalia found in the bags. Even after being arrested and paying bail, the suspects continued to partake in drug related activities and the process started over again (*California v Greenwood* 37-8).

The Supreme Court's majority opinion, written by Justice White, argues that trash bags left on the side of the curb reflect no reasonable expectation of privacy. Any individual or animal could easily go through the trash; therefore, it seems ridiculous to stop police from accessing what any member of the public can access (*California v Greenwood* 40-1). On the other hand, in a dissenting opinion, Justice Brennan argues that trash does carry a reasonable expectation of privacy. He begins his dissent by pointing out that the trash bags were opaque and sealed (Ibid 45). The incriminating items were not in plain sight spread across the defendant's lawn or the street in front of his house; if they had been, then there would be no expectation of privacy (Ibid 53). According to Brennan, if one applies precedent, those bags are protected because other non-see through materials, such as brown paper bags, a locked footlocker, and a zippered bag, all come with equal privacy expectations (Ibid 48).

GPS Technology and Privacy

Within recent years, the Supreme Court has decided cases several times that deal with the relationship between privacy and technology used in criminal investigation. *US v Jones*, decided in 2011, dealt with GPS tracking devices. Using suspicion of drug trafficking, police were able to obtain a warrant to install a GPS device on Jones's car. The key detail here was that it needed

to be attached within ten days; however, they did not attach it until the eleventh day. After about a month of surveillance, the government was able to convict Jones of the charges. On appeal, an Appellate Court invalidated locations while Jones was at his home because there was an expectation of privacy. However, they allowed the location evidence for when he was driving because there is no privacy expectation while utilizing public roads (*US v Jones* Syllabus 1).

The Court unanimously upheld the decision of the D.C. Court of Appeals (that the GPS tracking in violation of a warrant was unconstitutional). In his opinion for the Court, Justice Scalia makes an important distinction. The Court had previously decided that a car travelling from place to place could not be granted a reasonable expectation of privacy. In addition, a visual inspection of the exterior of a vehicle was also acceptable. However, the key difference in Jones's case was that there was no simple visual inspection. Investigators physically attached a device to the car with the intention of watching his movements (*US v Jones* Majority 9). In addition to the legal reasons the search was unallowable, the warrant expired before the device was attached to the vehicle, so it was already illegal.

In a concurring opinion, Justice Sotomayor reaffirms a crucial point introduced by Justice Scalia. As a reminder, in *Katz v US*, the idea that a physical trespass was needed in order to violate privacy was replaced with an alternate test of reasonable expectations of privacy. However, in no way did this decision completely eliminate the trespass rule. Using the most basic definition, if law enforcement breaches private property, they are conducting a search. The law still prohibits that action unless a warrant has been appropriately procured (*US v Jones* 2). Sotomayor continues her argument by stating the fact that GPS devices are capable of pinpointing a precise location; every single place, desirable or not that an individual went could

be recorded and stored (Ibid 3). If the Court had not chosen to restrict this action, the power to use GPS devices could have been greatly abused and utilized for almost any reason.

Cell Phones and Search Warrants

A different Supreme Court case, *Riley v California*, decided in 2014, deals with law enforcement access to cell phones. During a routine traffic stop, Riley's phone was accessed and the police officer discovered the regular usage of keywords often associated with gang activity. Riley was arrested and convicted of a shooting based upon video evidence that a detective found while searching his phone. A move to suppress the phone-based evidence was denied by two different courts so the Supreme Court agreed to rule on whether or not cell phone searches without a warrant violated privacy rights (*Riley v California* Syllabus 2).

In a unanimous decision, Chief Justice Roberts wrote the majority decision ruling that warrantless searches of cell phones were unconstitutional. To set a framework for analysis, Roberts first summarizes the decisions of three previous cases. One, *Chimel v California*, determined that there are two exceptions to needing a warrant for searching during an arrest; officers are allowed to search the person and their immediate surrounding space for weapons or anything else that could cause harm, as well as confiscating any piece of evidence that could potentially be destroyed. However, neither one of those two criteria is present when looking at digital cell phone evidence (*Riley v California* Opinion 6-9). As Roberts states, the data stored within a phone cannot be used to harm the investigating officer; however, they are free to search the exterior of the phone in order to ensure there are no weapons present. With regard to destruction of evidence, the United States failed to provide sufficient proof that there was a significant fear that a third party would remotely erase all data from the cell phone. There are

also several ways to avoid this issue, such as disconnecting the device from any cellular networks (Ibid 14).

Another important aspect of Roberts' argument centers on the storage capacity of cellular devices. Instead of only having access to a few pieces of physical evidence, if the police were to have access to an entire phone, there would likely be negative implications. They would have access to virtually a person's entire life; people store photographs, text conversations, and a wide variety of personal and sensitive information on phones (*Riley v California* Opinion 17). Much of this likely would not be of relevance to the investigation or crime but if warrantless searches were allowed on phones, it would be far too easy for law enforcement to take advantage of that privilege.

However, like any restriction, there are also exceptions to always needing a warrant for a cell phone search. If the police officer were to come upon a situation where the circumstances told them that there was a possibility of someone remotely erasing data or that they had an unlocked phone (both are incredibly rare circumstances), then they would be able to access whatever was necessary to examine the contents, or to remove the password (*Riley v California* 12-3). This is an important exception, because while it seems very unlikely to happen, the police have the authority in an emergency situation to investigate the contents of the phone without violating an individual's privacy rights.

Although not a Supreme Court case, only a few years ago there was another example of a similar phone search case. After a mass shooting in California in 2015, the FBI confiscated the shooter's phone. They were trying to gain access to the iPhone but the issue was that Apple built in a security feature; if too many wrong passcode attempts were tried, all data would have been erased (Khamooshi). Without this data, the FBI would not have been able to access information

that could have greatly improved the strength of the government's case. However, Apple's main argument was that if they were forced to create a backdoor into that particular iPhone, it would have created a security threat because other law enforcement or potentially other countries would have access to virtually any iPhone. On the other hand, the government argued that it was a national security matter; if they were successful on the San Bernadino case, it could prove to be a useful tool in investigating other terrorist attacks (Ibid). The case was eventually dropped when the FBI stated that a third party had assisted them with finding an alternative route into the phone.

Despite the fact that the case was never completely seen through, it still provides an important look into the principles created by *Riley*. Courts were not willing to force Apple to allow access into the phone because there was no established legal precedent in this specific area.

One final Supreme Court case that deals with cell phones in an investigation is *Carpenter v US*, decided in 2018. Unlike the previous two cases, *Carpenter* does not deal with physical access to a cell phone. Instead, it looks at the constitutionality of cell phone triangulation (a digital location technique) without a warrant. The circumstances of the case involve an investigation into a series of electronics store robberies. Four individuals were arrested and one confessed, even providing cell phone numbers for some of his associates. The FBI then used the Stored Communications Act to obtain cell phone records for several of the named individuals, including Carpenter. Using location data obtained from the service providers, Carpenter was arrested and convicted for involvement in several of the robberies (*Carpenter v US* Majority 3). Carpenter's argument for suppression of the location data centered on the fact that a warrant was not actually issued, because there was no probable cause. At a prior appeal, that argument was

denied on the grounds that, when Carpenter voluntarily shared locations with his cell phone provider, he forfeited his reasonable expectation of privacy (Ibid 4).

Previously, in *Miller v United States* (decided in 1976), the Supreme Court had created the "third-party doctrine". That case had centered on Miller's bank records which had been seized as part of an investigation into whether or not he was paying a liquor tax. The Court decided the records had been seized legally because Miller had no reasonable right to privacy of his bank records. They were part of the bank's business documents, not Miller's personal papers (*US v Miller* 435). This idea makes up the third party doctrine: any information voluntarily given to a third party has no expectation of privacy (Ibid 444).

However, unlike *Miller*, where the records had been voluntarily given to the bank simply by using it, the third-party doctrine did not apply to *Carpenter*. Similar to the logic given in *Riley*, if a law enforcement agency gains access to cell phone location data, they have access to everything. The government could track an individual's location everywhere, from the grocery store to religious services. The Court ruled that this violated Carpenter's expectations of privacy throughout his life because much of the location data found had nothing to do with the criminal investigation at hand (*Carpenter v US* Majority 12-3). Another important point in this decision was that sending cell phone location data was technically not voluntary; every time an individual moved, his phone automatically recorded location data, even though the person never explicitly consented to it (Ibid 17). Although this decision was a narrow one, specifically tailored to the case at hand, the Court refused to give the government unrestricted access to details of a person's entire life, an important step in the process of protecting the rights of an individual's digital privacy.

Still, this was a close 5-4 decision, so there are several dissenting opinions. Justice Kennedy points out that this decision was a break from precedent. He argues that cell phone records were the same as other types of government records that were allowed to be collected without a warrant, such as bank records and credit card statements. The government had used the appropriate procedures in each case so he questions why the process was not acceptable for cell phone records. In other cases, the Court found that the individuals did not own those records because they were kept and maintained by the actual companies. For this reason, Carpenter should not have had an expectation of privacy (*Carpenter v US* Dissent 2).

Justice Alito argues something similar in his dissent; he draws a distinction between a search and someone going through his papers and providing the necessary documents. In this case, it was just a business going through its documents. A major departure from precedent occurred from the Court's ruling in *Carpenter*. The "Court allows a defendant to object to the search of a third party's property…The Fourth Amendment protects 'the right of the people to be secure in *their* persons…not the [things] of others" (*Carpenter v US* Dissent 15-6).

While there are definitely major drawbacks to allowing the government full access to an individual's location data, it does not seem right that the Court should vary from precedent set by similar cases involving comparable circumstances. Even though Carpenter paid for a cell phone plan with a specific carrier, that did not mean he then has ownership of his phone's data records. They became the property of the cell phone provider when Carpenter signed up with the firm.

Constitutional Privacy in a DNA Context

One of the more well-known Supreme Court cases dealing with the constitutionality of DNA collection practices is *Maryland v King*, decided in 2013. This case looks at the

acceptability of the Maryland DNA Collection Act, which allowed law enforcement to take a DNA swab after the arrest of anyone charged with a felony and compare it to other samples in a criminal database. King was arrested on first and second degree assault charges, so a DNA swab was taken (*Maryland v King* Syllabus 1). The issue arose when King's DNA matched an unsolved rape case from years earlier; he was convicted but a higher court overturned the decision. This court stated that permissibility to collect DNA from felony arrestees was unconstitutional because the individual's expectation of privacy outweighed the desire of the government to protect its citizens by finding the culprits of crimes (Ibid 2).

Justice Kennedy wrote the majority opinion in this case; it overturned the lower court's ruling and stated that it was constitutional for law enforcement to collect DNA from individuals arrested on felony charges. However, the key point Kennedy makes is that the DNA can be used for identification purposes only (*Maryland v King* Majority 5). A swab gathering cells from the inner cheek is a search (so it is still protected by the Fourth Amendment), but it is not an intrusion in the way that drawing blood is (Ibid 7-8). Arrestees do not have the same expectations of privacy that other people have. For example, after being taken into custody, a suspect may be required to undergo an extensive search of his person; in some cases, this can include the suspect stripping naked and having every inch of his body checked for contraband (*Maryland v King* Majority 25).

In addition, it is absolutely crucial for police to have identifying information for suspected criminals, including their past criminal records. They must know if there are any serious threats presented by these individual, such as a security risk, in order to ensure that the lives of both corrections officers and the public are protected. The widespread acceptability of DNA identification is basically the same thing as "matching an arrestee's face to a wanted poster

of a previously unidentified suspect" (*Maryland v King* Majority 18-19). In addition to identification prior to court proceedings, the sentencing judge needs access to things like criminal history in order to develop an appropriate sentence, or to determine if the suspect can be released on bail (Ibid 14).

On the other hand, Justice Scalia contributed a powerful dissent to this case. He argues that the Court is wrong because it misinterpreted the main point of running the data through DNA databases with samples from unsolved crimes. The majority opinion appears to assume that previous criminal history obtained from matching unsolved cases to the suspect's DNA is for the judge's use during arraignment and bail proceedings. However, as Scalia points out, King's DNA was not processed until after the arraignment. He goes as far as questioning whether his fellow Justices actually believed that Maryland did not know the name of the defendant (*Maryland v King* Dissent 7).

For Scalia, the primary purpose of using DNA to identify a culprit is to confirm a suspicion, not to explore a random possibility. He uses the example of stopping cars to demonstrate this principle. A police officer is not going to stop every single car on a highway to look up the criminal records of drivers in hopes of discovering warrants for the arrests; no rational court would be willing to say that was legal (Ibid 5-6). By that logic, the Supreme Court should not agree that looking up DNA in a database, in the hope that unsolved crimes can be attributed, can be legal either. Justice Scalia adds that "King was not identified by his association with the sample; rather, the sample was identified by its association with King" (Ibid 9). This is not identification as the Court majority purported; it was pure optimism.

Many legal scholars agree with Scalia's dissent. One, David H. Kaye, agrees that the Court's emphasis on using the DNA sample for pretrial purposes of identification seemed

irrational. Justice Kennedy did not argue that having a DNA sample was a valuable piece of evidence; instead, he insisted the only value it added was before the trial occurred (Kaye 546). However, Maryland's law stated that without permission, the DNA could only be used for identification purposes (Kaye 549). Thus, running the DNA through a database, specifically looking for other matches that do not relate to identifying the individual, is a clear violation of the law.

What are the Arguments For and Against?

Prior to engaging in a deeper analysis of the acceptability of partial familial matching, it is first crucial to note that none of the individuals mentioned in the Supreme Court cases discussed above were exemplary citizens. Therefore, they should not be looked up to as role models. However, due to the fact that they are American citizens, they are guaranteed certain rights by the Constitution. These rights include a protection of "unreasonable searches and seizures" found in the Fourth Amendment.

Arguments for each side can be categorized into three more general points. On the side of arguments supporting partial familial matching, these include: making the job of law enforcement easier, solving cold cases, and the belief that privacy rights are waived as soon as something enters the public sphere. The opposing position, with arguments against partial matching, includes a desire for minimal government intervention, irrelevant information gathering, and the issue of consent. Each of these arguments, whether for or against, is supported by principles from a Supreme Court case mentioned above.

Argument For: Making Law Enforcement's Job Easier

One of the main arguments in support of familial matching as a criminal investigation technique is that it makes the job of law enforcement much easier. This is seen by the Court's argument in *Maryland v King*, when Justice Kennedy insisted that the cheek swabs would only be used in the investigation of serious violent crimes. Maryland had specifically defined those crimes as including but not limited to: "murder, rape, first-degree assault… [and] sexual assault" (*Maryland v King* Majority 4). The crime for which King was arrested was first-degree assault, which counted as a violent crime under Maryland law. For this reason, it was acceptable for the cheek swab to be taken. DNA was not being extracted from random criminals, but only from suspects that posed a serious safety risk. If a cheek swab, a minimally invasive procedure, could be done to solve serious crimes, then arguably, familial DNA testing should be allowed when investigating cold cases involving rape and murder, among other crimes.

The second major piece of this argument in Justice Kennedy's *King* opinion agrees with the argument brought forward by the United States government; it is crucial to know about the arrestee's history in order for proper safety measures to be carried out. If an individual was detained for a minor offense, it is entirely possible the individual is actually guilty of a much larger, nefarious crime. Kennedy uses the example of the notorious Oklahoma City bomber, Timothy McVeigh; a trooper realized he was driving without a license shortly after the bombing took place (*Maryland v King* Majority 12). Using the same logic, it is plausible that an individual stopped for traffic violations or another minor crime could actually have previously committed murder or armed robbery. According to Kennedy's opinion, unless there was a method to see an individual's history, police and corrections officers would likely not be adequately prepared for any special safety measures that needed to be taken. A judge needs to

know the individual's background, criminal history, and flight risk in order to properly set bail or determine if the individual must be held without bail (Ibid 15). DNA is just another investigative tool that can ensure each of these safety concerns is sufficiently and appropriately addressed.

The second case that deals directly with the potential to make law enforcement's job easier is *Kyllo v US*. In his dissenting opinion, Justice Stevens argues that inferences are not illegal. In this case, the officer was measuring the heat exiting the house; the device he was using to do so only provided a heat signature (*Kyllo v US* 28). Furthermore, the thermal imaging device did not provide a neat printout automatically identifying that Kyllo was growing marijuana plants. Having some knowledge about heat signatures, police were able to infer the suspect was likely growing the plants. As Stevens writes, "[i]t would be quite absurd to characterize [the officers'] thought processes as 'searches'" (Ibid 44).

Even if the use of the thermal imaging device did count as a search, labelling inferences as searches would mean that many forms of traditional police work would not be allowed. The application of Stevens' logic to the topic of familial searches suggests that running the genetic information through a database would be allowed; even after the police obtained any potential matches, they would still need to carry out traditional investigations in order to infer who the culprit was. Similarly to the heat device, partial genetic matching does not spit out a neat little image of who the culprit is.

Argument For: Solving Cold Cases

Arguably the most well-known American case involving DNA ancestral searches is that of the Golden State Killer. As a reminder, this criminal was a serial killer with countless rapes, murders, and burglaries attributed to him. He terrorized the state of California between 1976 and

1986 before going dormant. This case soon went cold because the killer was constantly evading capture. In several instances, the police were close to capture, and even encountered the suspect, but they did not realize at the time that he was the serial killer. Finally, a break in the case came when investigator Paul Holes searched for a match on GEDmatch, an online, public ancestry website; a partial match appeared (Lussenhop). The profile belonged to a 73 year old man living in Oregon. In April 2018, after decades of painstakingly searching for answers, Joseph James DeAngelo Jr, a former police officer, was arrested (Brown). After the apprehension of the Golden State Killer, law enforcement around the country was willing to use this cutting-edge technique in an attempt to solve some of the toughest cold cases.

A similar case began in 1992, when a woman was murdered in Lancaster, Pennsylvania. However, due to a lack of leads, the case went cold a few years later. After hearing about the success of using a public genealogy website in the Golden State Killer case, investigators thought it might work in this situation as well. A match was found after a company called Parabon offered to help; a relative of the suspect, Raymond Rowe (or DJ Freez), had uploaded their genetic profile to GEDmatch (Woods). After using traditional investigative techniques, police were able to track Rowe to a DJ event he was working and obtained a water bottle that he threw away in a public trash can to test for DNA evidence. DNA tests showed that the sample taken from the water bottle matched samples taken from the victim's body (Ibid).

A final example occurred more recently from 2006-2008 in Fayetteville, North Carolina. A man referred to as the "Ramsey Street Rapist" committed dozens of sexual crimes and burglaries. Police were unable to find any successful leads and the community became increasingly more fearful as time passed and no perpetrator was found. However, Parabon, the same company that was used in the Lancaster case, offered to assist law enforcement agencies in

using online ancestry databases. Parabon gave police a strong list of potential matches that they were able to narrow down to find one suspect. The individual who was arrested was a forty-three year old man who was born and raised, and still lived in the area where the crimes were committed (Fortin). Had Parabon not offered the service to local officers, or if police had not found a match, this man would still be walking around in the community that he had terrorized.

In addition to solving cold cases, the usage of familial DNA searches can also help exonerate individuals. One case that demonstrates this is the 1996 murder of Angie Dodge in Idaho; despite having DNA found at the crime scene, a search of a national crime database did not give any definite matches (Mustian). A later search of Ancestry.com came up with a partial match and a court order required the website to release the individual's name. After narrowing the search down from several generations of potential suspects, the police discovered only one who could have been a possible suspect. Michael Usry, a New Orleans filmmaker, was known for making graphic, violent films, so the police closed in on him. A judge signed a search warrant, allowing police to obtain Usry's DNA and he was forced to live in fear of what could potentially happen. Eventually, DNA testing proved his DNA did not match the suspect (Mustian). The police would not have discovered Michael Usry could be a potential suspect without the usage of familial DNA searching. Fortunately, they were able to realize he was not the culprit after testing. Police could now follow other leads and stop investigating an innocent man.

Argument For: Entering the Public Sphere Forfeits Privacy

This principle is addressed by two specific Supreme Court cases. The first is *Olmstead v US*. While this case is not very recent, one of the issues at hand was whether or not the phone

lines were considered to be private. In his majority opinion, Chief Justice Taft writes that a search can only occur with regard to tangible, material items. Due to the fact that the item in question was spoken conversation, there was no search done, according to the Court (*Olmstead v US* 464). A simple rebuttal to this argument would be that listening to the conversation infringed on Olmstead's right to privacy, under the Fourth Amendment because he was making the calls from inside a home and a private office.

However, Taft goes further and states that it is reasonable to expect the physical telephone to be private, but that the telephone wires are not because an individual having a phone conversation knows his voice will be projected over a far distance (Ibid 466). Taft states, "The language of the Amendment cannot be extended and expanded to include telephone wire reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched" (*Olmstead v US* 465). An individual owns the specific telephone that he uses to speak into but not the phone lines transmitting that conversation.

The second Supreme Court case looking at privacy within the public sphere is *California v Greenwood*. As a reminder, this case determined that an individual could not have a reasonable expectation of privacy with regard to trash bags once they were put out on the curb for pickup. In his majority opinion, Justice White writes that searching trash bags without a warrant is only a Fourth Amendment violation if society feels there is a reasonable expectation of privacy (*California v Greenwood* 39). Putting the bags on the curb was enough to convince White that there could be no reasonable expectation to privacy in this case. "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" (Ibid 40). Due to the

fact that anyone could theoretically search through one's trash, there cannot be a granted notion of privacy in this scenario.

There is no reason to regard trash bags as the private property of the individual who filled them and discarded them on the side of the curb. It would be somewhat preposterous to assume that individuals putting their trash bags on the side of the road have a reasonable expectation of privacy forever. Once picked up, the bags intermingle with other peoples' trash bags and they all end up in a landfill. While en route, trash bags can break open and have items spill out. People searching at a landfill may dig through the bags in search of a specific item and can do so without having to worry about infringing on one's property rights; therefore, it makes little sense to restrict searching bags meant to be thrown away.

Argument Against: Potential for too much Privacy Invasion

Despite seemingly concrete arguments for supporting the use of partial familial searches, the arguments against these searches also provide a myriad of questions regarding the acceptability of the practice. The first argument is that the government should not be allowed to intervene unnecessarily in the lives of citizens. With specific regard to this issue, the fear is that if police are allowed to investigate individuals who are not actually suspects in a crime, then eventually, the authority and purpose of the Fourth Amendment will be undermined.

This concept is explicitly discussed in Supreme Court Justice Antonin Scalia's powerful dissent in *Maryland v King*. The Maryland DNA Collection Act (the law in question in this case) stated that the only reason DNA could be collected from an arrestee was for purposes of identification. However, for King, his DNA was not used to determine who he was. The law stated that DNA could not be processed until arraignment; for King, the search occurred three

days after his arrest. The sample was not sent for testing until almost three months later. It was not until four months after his arrest that King's DNA results were run through the national DNA database (*Maryland v King* Dissent 6-8). As Scalia writes, "Does the Court really believe that Maryland did not know whom it was arraigning?" (Ibid 7). The test results were entered into Maryland's database with identifying information so clearly King's identity was known. It took four months for the results to come back. If the purpose really was to determine a suspect's background and criminal history, the sample would have been tested much faster than it was.

Additionally, it is quite clear that the purpose of the search was not to identify the suspect. The DNA was put into the national unsolved crimes database, not the one for known convicts and arrestees' one (*Maryland v King* Dissent 8-9). Furthermore, Maryland law prohibited using DNA for any purpose other than identifying human remains or missing people (Ibid 11). Obviously, King was neither a missing person nor a set of human remains. Finally, in the majority opinion, the Court attempts to argue that fingerprints and DNA serve the same purpose. However, this is drastically incorrect. As Scalia writes, fingerprints are used to identify individuals and DNA is taken to solve crime (Ibid 14). Based off of this information, the state of Maryland had no legitimate grounds to use King's DNA for purposes of "identification". Ultimately, each piece of Justice Scalia's dissent culminates in the main point that "King was not identified by his association with the sample; rather, the sample was identified by its association with King" (Ibid 9).

The police had literally no reason to assume that King had previously committed a crime; the Fourth Amendment protects against "unreasonable searches and seizures," especially suspicionless ones. Unfortunately, this issue is not one that began only with King's case. It goes all the way back to the beginning of America. Several of the Founding Fathers had strong

opinions about the issue of criminal rights. During Virginia's Ratifying Convention for the Fourth Amendment, Patrick Henry spoke against general warrants and said, "As these are admitted, any man may be seized; any property may be taken, in the most arbitrary manner, without any evidence or reason. Every thing the most sacred, may be searched and ransacked by the strong hand of power" (Henry). Without protecting against random and arbitrary searches void of probable cause, individual liberties and rights will be taken from citizens of America. Seen then and now, unless restrictions are placed, there is nothing stopping law enforcement from using the idea of search and seizure whenever they want, and for whatever purposes they want.

Argument Against: Too Much Access to Irrelevant Information

One common argument that is seen throughout many of the Supreme Court opinions previously discussed is the need to prevent law enforcement from gaining access to information that is irrelevant to the case at hand. The first exploration of this argument occurred in 1988 in Justice Brennan's *California v Greenwood* dissent. He writes that digging through another's trash bags has never been a socially acceptable action because it goes against "commonly accepted notions of civilized behavior" (*California v Greenwood* 45). Privacy within opaque materials has already been recognized several times before; the same protections are found in everything from a brown paper lunch bag to a padlocked footlocker (Ibid 48). Additionally, garbage bags are often used as an easy way to transport various items; there should still be privacy protections for them (Ibid 49).

A search through someone's garbage bags can reveal a wealth of information about the occupants of that address. Digging through trash can reveal hobbies, socioeconomic status,

family life, religion, and health, among countless other details. It is very likely that these items would not aid in a criminal investigation (*California v Greenwood* 50). During the search through Greenwood's trash, the officer inevitably found other items with zero relevance to the narcotics investigation.

An incident involving Henry Kissinger's garbage demonstrates several of the fears seen in Brennan's opinion. Although it was not a police investigation, a freelance tabloid reporter searched through Henry Kissinger's trash for an article. The reporter discovered many sensitive documents during his search. The public was outraged because they saw it as an unreasonable invasion of privacy (Ibid 52). Had Kissinger been under investigation for the same crime as Greenwood, the sensitive material found in his trash would not have been related to the investigation, yet the police would have learned about potentially sensitive government operations. The police should not be searching through another's trash without probable cause and a warrant due to the harm that can come from knowing about another's lifestyle or having unauthorized access to sensitive content.

A second instance in which this principle is shown is by the 2001 case, *Kyllo v US*. Scalia begins his opinion for the Court by reminding readers that in *Katz v US,* wiretapping was declared unconstitutional because Katz's actions once in the phone booth clearly showed he expected privacy, and wiretapping infringed on that privacy (*Kyllo v US* 33). The dissenting opinion attempted to make the distinction between "off the wall" surveillance (gathering evidence outside the home) and "through the wall" surveillance (evidence inside the home). However, as Scalia correctly points out, that distinction is ridiculous. The entire home is safe from government invasion so gathering information beyond what one could see in plain sight still violates the privacy of the home. In *Katz*, wiretapping only sound waves that reached the

exterior of the phone booth was struck down. Using the same logic, Scalia determines that gathering signatures from heat that escapes a home is also not permitted (*Kyllo v US* 35).

Additionally, based on the information found by a thermal imaging device, it would be all too simple to determine an individual's daily schedule. For example, an officer could determine when members of the family bathe, cook, or turn on a closet light, among countless other daily tasks (Ibid 38). In this specific case, none of those intimate details would tell police anything about whether or not marijuana was being grown inside the home; the same would likely be true for most other cases.

A third case that has nothing to do with the home yet still makes the same point is *US v Jones*, decided in 2012. In opinions that concurred with the Court's unanimous decision, both Justice Sotomayor and Justice Alito make similar points about the idea that GPS tracking can essentially map out one's movements. Similar to the arguments addressed above with regard to determining someone's daily schedule from evidence obtained within the home, GPS tracking could reveal what businesses or religious establishments an individual goes to; this could tell a great deal about that person's interests, health conditions, and shopping habits (*US v Jones* Concurring 3). In his opinion, Alito states that new technology within toll booths and cars themselves can allow law enforcement to create a precise map of where an individual travels each day (Ibid 11). With regard to either one of these techniques, "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse" (Ibid 3). Without restrictions on the government's power, it could easily decide to track an individual without reason.

Riley v California, decided in 2012, moves the focus of the issue from basic technology to the plethora of information that can be found on a cell phone. In the unanimous decision,

Chief Justice Roberts writes that smart phones "could just as easily be called cameras, video players…calendars…diaries…maps, or newspapers" (*Riley v California* 17). Due to storage capabilities, virtually anything can be stored within a phone or an app on it. A sixteen gigabyte phone can store millions of texts or thousands of pictures and videos (Ibid). New apps are constantly entering the market and cover basically every aspect of a person's life-from entertainment to news to education. Being able to access a phone means everything about someone is accessible, right there in the palm of the officer's hand. Instead of having to search through an entire house or vehicle, the officer can find information about anything, including things such as medical history, schooling, interests, and family life. As with each of the situations mentioned above, it is virtually impossible to think of a case where every single piece of information on one's cell phone would be pertinent to a criminal investigation.

Another point discussed in Chief Justice Roberts' opinion, revolves around the idea that an arrestee has fewer privacy expectations that a non-arrested individual but that in no ways means he is required to give up all rights to privacy. In a somewhat similar case, *Chimel v California*, decided in 1969, it was ruled that police cannot search through an individual's entire residence when arresting the person because only items on the person and within reach could cause immediate harm to an officer (*Riley v California* 6). Another case, *US v Robinson*, determined that for searches incident to an arrest, it needed to be decided on a case-by-case basis if the officer was at risk of harm or if evidence was at risk of destruction (Ibid 7). The Court then needed to determine how smartphones fit into this rule. With any arrest there is always a risk of harm to the officer. However, with digital information, there is no risk of physical harm to the officer, and there is negligible risk of any evidence being destroyed. Therefore, there is no

allowance for searching a cell phone without a warrant; too much personal information is at stake and there is no risk of harm.

The final case that discusses the idea of access to irrelevant information is *Carpenter v US*, decided in 2018. It incorporates aspects of several of the previous cases in that it involves both cell phones and location tracking technology. Due to the fact that in today's society, humans are basically attached to their phones, Chief Justice Roberts writes that cell phones are "almost a 'feature of human anatomy'" (*Carpenter v US* Majority 13). Cell phones have very precise location tracking, almost as if the phone were an ankle bracelet (Ibid). Cell phone triangulation allows a fairly specific map of one's location to be created. If the government is allowed unrestricted access to this information, it can see each location an individual went into and at what time; as with the other cases, this practice would allow sensitive information to be gathered (Ibid 12-13). As technology becomes more advanced and more cell towers are built, location tracking becomes more and more precise. One day, technology may allow police to determine the precise location of each and every individual (Ibid 14-15).

All of these cases show the major concern that law enforcement officials can get access to far more information. After finding a partial match through the use of familial DNA searches, law enforcement must use traditional investigative techniques to narrow down the suspect pool. However, through the course of investigation, the police could gain access to a wealth of material not relevant to the case. This can be seen through the above descriptions of information that can be accessed through various technologies.

Argument For: Issues of Consent

Within the overall issue of consent, there are a few specific subsections that must be discussed. The first is that just because one family member puts his or her information on a public genealogy website, it does not mean that the rest of the family does as well. University of Baltimore Professor Natalie Ram states, "Identifiable genetic information is shared among these relatives as an involuntary product of biology, not consent" ("DNA by…" 925). An individual who never gave consent can be identified, investigated, and even arrested based solely on the fact that a relative uploaded information to a public database (Ibid 877). If one individual uploads their information, he gives consent for his profile to be used; this is not consent for family members. Although not about DNA, a similar idea regarding consent that Natalie Ram uses is property ownership. If two or more individuals jointly own a piece of property, nothing can occur without the consent of all owners; one owner cannot decide to start changing or selling off pieces of the property and assume that the others automatically consent (Ibid 920).

An example of this concept is demonstrated by a 2014 conviction where the culprit was identified based on familial searching. Virginia police had been able to determine that three crimes were connected to the same culprit but were not able to figure out who the primary suspect was until the state forensics unit was able to find a partial match in the state's DNA database. The DNA belonged to Kenneth Holloway, a man with a criminal record who had not been in jail for over ten years. Using traditional techniques, police were able to narrow the search to Holloway's brother, Tyrone. After testing a sample from Tyrone, police determined that his DNA matched samples taken from the crime scene; they were able to convict him ("DNA by…" 875). Kenneth Holloway later said that he felt the police should not have used his DNA the way that they did. He "understands that because he is a felon, authorities have a right

to his DNA should he ever reoffend… [However,] he feels it was wrong to use [his DNA] to go after his brother" (Ibid). Consent for DNA is not just a random, arbitrary principle created by those against the use of familial searches; people do not want their DNA used to implicate others who have not consented.

Another hypothetical example of consent is a common practice when an individual goes on a cruise. Individuals must sign a waiver stating that any photographs taken of them while on the cruise can be used for promotional purposes. If one individual signs the waiver but his accompanying sister does not, then any picture including both of them cannot be used by the cruise line. The consent (waiver) signed by the first person does not automatically extend to the second relative even though they are in the same family.

Similarly, the government does not have the authority to determine who gives up or forfeits consent. As mentioned above, one does not choose the relatives with whom they share DNA; likewise, they do not choose what specific traits they share with those same relatives ("DNA by…" 904). Family members also do not control the actions of other family members. Logically, it then follows that if one relative commits a crime and is required to give up certain privacy rights, such as having his genetic profile included in a national crime database, the government only has legal access to that specific person's information. The judiciary should establish a rule stating that the government can only search DNA from an individual who has either uploaded DNA to a public database, consented to the search, or been legally ordered to do so (Ibid 921-3).

Blood relatives are always going to share some DNA simply due to the fact that they are related. This does not allow the government to determine for the entire family who gives up rights just because they may have access to a portion of each family members DNA (through the

one profile the government has). This concept can also be explored using the previous analogy of home ownership. Say the owner of one apartment in an apartment complex of 200 homes consents to let law enforcement search their home. Once police are done with that apartment, they decide to go and search the other 199 apartments in the complex because the first owner gave consent. According to the government's logic, this would be acceptable because one owner consented and the similarity between all the apartments is that they are part of the same complex. However, there are a myriad of Supreme Court cases and the Fourth Amendment itself that declare searching dwellings without consent or a warrant is unconstitutional. This same principle should apply to families; one does not get to consent for all.

The final crucial piece of consent to be looked at is what the actual public ancestry websites say. Ancestry.com and 23andMe each have a clause in their privacy policies stating that a user's DNA may be provided to law enforcement; the companies each say they would usually only do this when necessary to legal processes, or to protect either a user or the company (Kase et.al., 8). GEDmatch, the database used in the previously mentioned cases, states in their privacy policy that DNA may be shared with police in order to help solve serious, violent crimes or to identify human remains (Ibid). With regard to Chief Justice Roberts' opinion in *Carpenter v US* and his point that cell phones are basically part of the human anatomy, some scholars feel that, if that is the rule being set forth, then DNA (an actual part of the human anatomy), should definitely receive the same protections (Ibid). This means no searching without consent.

One essential piece of information to note pertaining to the privacy statements of these firms is that they never state that a family member's information can be shared, only the individual uploading their DNA. Thus, it is easy to assume that the websites can only share one DNA profile because that individual is the only one consenting. This is not to say that no one

should ever be using online genealogy websites; they can serve a valuable purpose in terms of finding family members or completing a family tree. However, one should not be required to have a family meeting in order to ensure every single member of the family is okay with potentially being investigated for a crime they may not have committed.

What Have States Already Done?

Now that the main arguments for both sides have been discussed, the next step is to look at what various states within the United States have done to address this practice. In 2008, California was the first state to allow partial matching to be used as a criminal investigation technique; however, public databases were not to be searched. Only the California's state DNA database could be used specifically for partial match searches; matches found through a routine search of the database were also permitted ("Fortuity…" 753). Colorado decided to follow in California's footsteps in 2010 (Ibid 755). In 2011, one study sought to determine what each state's policy was regarding partial familial searches of the state databases. It discovered that only two places, Maryland and Washington D.C. had formally prohibited intentionally searching the database for partial matches (Ibid).

On the other hand, Colorado, Nebraska, and Texas all have regulations stating that all other potential investigative leads and techniques must be attempted before partial familial matching may be used. These three states, in addition to California, were the only four in the study to allow both routine and intentional partial matches. Each of these states has guidelines outlining when partial matching is allowed. An unsolved case must pose a severe public safety threat or be a serious violent crime; according to Texas, crimes such as homicides or sexual assault would fit into this category ("Fortuity…" 781). Texas goes further in its strict

regulations, stating that the evidence must be a complete genetic profile from one individual, or no contamination (Ibid).

Many of the states allowing partial searches also require some form of genetic testing prior to the search in order to determine if there is a likelihood that the two samples could belong to relatives. However, these states vary in the minimum number of shared alleles (or specific points in the DNA) to warrant the search. In the case of North Carolina, the only DNA results that are officially considered to be a match are those where the alleles present in each sample are identical; lab technicians are allowed to informally provide information about partial matches to investigators ("Fortuity…" 782). On the other side of the spectrum, in 2011, some states did not have a policy regarding this type of investigative technique. Others had a policy but it was either considered a sensitive document or it was locked away in an internal lab manual; in both cases, it is incredibly difficult to access the policies as they were not available to the public (Ibid 776).

What Do Other Countries Think About Genetic Privacy?

In this section, three countries will be discussed: the United Kingdom, Japan, and Germany. Each of these countries has a unique culture and system of values that is different from one another, as well as from the United States. Therefore, it is likely that none of these systems should be identically implemented in another; however, important lessons can still be learned.

The first country to be explored is the United Kingdom. Unlike the United States, the United Kingdom gives a great deal of power to its law enforcement when it comes to crime solving techniques. In 1995, the country created the National DNA Database (NDNAD). Between the database's creation and 2008, the British Parliament passed a series of legislative

acts that slowly expanded the power of law enforcement to "obtain, store, and access biological samples and DNA profiles" (Krimsky and Simoncelli 169). Under these laws, the police are allowed to store a DNA sample indefinitely, even if the individual was never charged with a crime. If someone is arrested for a crime, the police do not need consent to take a DNA sample (Ibid 170).

The United Kingdom is often the leader in terms of new investigative techniques using DNA. As previously mentioned, in 2004, the country was the first to use familial DNA searches to secure a conviction. Between that case and 2008, Britain used familial searching as a technique in 148 cases; fifteen positive matches came back and nine convictions were obtained (Krimsky and Simoncelli 175). In addition, the United Kingdom is the only country to regularly use this investigative technique in high-profile cases (Ibid). Clearly, this country has fewer privacy protections than the United States, so it is unlikely that this technique can ever be implemented here.

The second country to be examined is Japan. In 2004, years after the United Kingdom created their National DNA Database, Japan did the same. Unlike the United States and the United Kingdom, Japan's practice of collecting DNA samples only allows for a sample to be obtained if DNA was found at the crime scene. DNA profiles are also regularly removed from the database after cases are closed or if the police feel there is no need to keep the profile any longer (Krimsky and Simoncelli 188). Although it may seem that Japan is very concerned with protecting the privacy of its citizens, each sample entered into the DNA database contains a large amount of sensitive material. For example, identifying information such as the name and birthdate of the suspect, as well as the arrest date and crime are included (Ibid 187). This aspect of the database makes it very controversial. However, recommendations were made in an

attempt to provide oversight; these included removing DNA profiles if the suspect was acquitted as well as after a set number of years (Ibid 190).

Despite the lack of regulation with regard to Japan's DNA database, the country's constitution provides some protection. Article 35 of the Japanese Constitution is very similar to the United States' Fourth Amendment and essentially states that no unreasonable searches and seizures are allowed. If a search is to be done, a specific warrant detailing the "place to be searched and things to be seized" needs to be issued by a "competent judicial officer" (Krimsky and Simoncelli 186). According to Japanese law, obtaining DNA without a warrant goes against Article 35. In addition, if the DNA is not essential for investigating the crime, collecting it goes against due process regulations of Article 31 (Ibid 190).

The final country to discuss is Germany, the privacy protections of which favor as little unnecessary government infringement as possible. For this country, the context behind their strict rules is crucial; during the time of Nazism and their eugenics movement (essentially selective breeding to create a desired race), countless groups were seen as inferior due to their ancestry and genetic makeup (Krimsky and Simoncelli 205). A very reasonable modern fear stemming from that era is that with a central DNA database, anyone with a nefarious plot could attempt something similar to what occurred in the mid twentieth century. However, after a few high profile cases of murder and sexual abuse, Germany realized that it could no longer survive without a DNA database; theirs was created in 1997 (Ibid).

German law outlines very specific regulations for obtaining and destroying DNA samples. Samples can only be obtained to identify a parent, or to attach an identity or gender to a crime scene sample. Unless the situation is one of informed consent or pertains to a crime scene sample, a judge must sign a warrant to collect and analyze DNA; that judge also acts as a

safeguard against conflicts of interest. He or she appoints the expert who will carry out the analysis; this expert must be able to ensure the results will not be accessible to any unauthorized party. Basic identification information for the sample is not allowed to be seen by the lab technician either (Krimsky and Simoncelli 208-9).

Guidelines are just as explicit when it comes to the removal or destruction of a DNA sample. As soon as any DNA profile is created (including convicts), the physical DNA sample must be destroyed. Germany is not alone in having very explicit, strict regulations for destroying DNA samples; countries such as Belgium, the Netherlands, and Norway have similar rules (Krimsky and Simoncelli 210). Within Germany, it is illegal to use DNA for any reason other than creating the profile. If the suspect is acquitted of the crime, the profile must be removed from the database. Finally, every ten years, all profiles within the database are reviewed to determine if there is any legitimate reason to keep them (Ibid). Based upon these restrictions, familial searches definitely would not be allowed; investigating someone without any reason to suspect them would violate their strict privacy rules. A judge would also not sign a DNA collection and analysis warrant because obtaining a sample from a seemingly random individual without cause does not comply with Germany's laws.

Due to the unique aspects of each country's culture, values, and history, privacy guidelines and approved investigation practices will be different. Every country has its own needs and desires which will be reflected in the laws and regulations of each nation. Although there may be good facets of each of the regulations discussed above, none of them will be perfect for the United States. This country would fall somewhere in the middle of Germany and the United Kingdom. Police in the United States do not have anywhere near as much latitude as British police but the country has looser privacy guidelines than Germany.

So Now What?

After examining what the arguments are and how various countries and states have dealt with the issue of whether or not partial familial searches should be allowed, the next logical step is to take all that information and determine what should come of it. Based upon the Supreme Court's hesitation to provide the government with wide-sweeping powers to get many forms of evidence, it does not seem likely that complete and total unrestricted usage of familial searches will ever be allowed. Too much information is gathered without cause and most of the implicated individuals never consented to allow their DNA to be used.

Although this technique can be useful in solving tough cases, including cold cases, the government should never be permitted to search without probable cause. Even in exigent circumstances or situations where a warrantless search is allowed, there is still some form of cause that allows law enforcement to carry out a search. In cases of familial searches, there is no probable cause, not even an iota of reasonable suspicion to investigate dozens of individuals. These individuals are at risk of having their lives ruined. When applying for a job or getting involved in a relationship, the person will need to explain that they were or are under investigation for a crime. Even if they did not commit it, society will likely wonder what evidence the police had that lead them to consider the individual a potential suspect; the probability of negative stigmatization will increase.

From a legal perspective, an entire case cannot be based solely on DNA results. It is not 100 percent foolproof, because human error or contamination can occur, despite extensive efforts to prevent mistakes. DNA can place someone at the scene of the crime but it cannot definitely prove someone is guilty without other evidence. For example, if someone on a run comes upon an individual who has just been stabbed, they will likely try to help. In the process, DNA in

sweat, hair, or skin cells can be transferred to the crime scene. The runner's DNA will likely show up on DNA tests, but that does not mean they committed the crime. Other evidence such as clothing fibers or security camera footage, among countless other examples, will need to be used in order to prove that someone is the actual culprit.

Finally, even though one is skeptical of or against the use of partial familial matching, it does not mean that they are automatically against law enforcement being able to solve hard cases. It means that someone is not willing to sacrifice protections guaranteed by the Constitution and the Fourth Amendment in exchange for making the job of police easier. Every restriction placed upon law enforcement by a Supreme Court decision prohibiting a specific investigative technique is not doing so solely to make solving cases harder; these decisions are made first and foremost to ensure that individual rights and liberties provided by the United States' governing documents are protected from unreasonable and inappropriate invasion by the government.

While putting more restrictions on the investigative techniques of law enforcement may make their job harder, it will make their work better. They will need to ensure that they have completely solid evidence before looking to get a search or arrest warrant. Restrictions will also hopefully ensure that fewer innocent people are investigated for crimes in an effort to find the actual culprit. This limitations could include restricting familial DNA searches to only the most severe of cases where no other technique has worked. A second major restriction needs to be that police must have probable cause to believe an individual from a specific family tree has committed the crime; they cannot be allowed to run samples through a database hoping a match will be found. Law enforcement also need to have probable cause prior to diving into an individual's life, even if they are in the same family tree as the original partial match.

One point of historical analysis is to learn from the past and apply those lessons to make the future better. Instead of ensuring that people in the future will be less apprehensive due to law enforcement following proper procedures, a lack of restrictions preventing unrestricted access to Americans' lives would be immensely detrimental and plunge society back into one of paranoia and fear, unable to function properly.

The Future of DNA and Privacy

There are two major issues relating to the future of DNA and genetic privacy. The first relates to the question of if legislation is needed to aid the future of genetic privacy and DNA databases. Some scholars feel that more restrictions need to be placed upon law enforcement in order to ensure that the individual's privacy is properly protected. Laws such as HIPAA and the Genetic Nondiscrimination Act of 2008 protect an individual's genetic data because there is strict confidentiality required (Ram et al. 2-3). Additionally, several public genetic databases allow law enforcement to access profiles in order to investigate certain serious crimes, such as murder. However, there is no equivalent law that restricts law enforcement; as of now, they are allowed to freely search databases without absolute knowledge that the individual they are looking for has voluntarily provided their profile (Ibid 3). The, state laws discussed above that restrict or allow partial DNA matching apply only to state or law enforcement databases. There are no laws that apply specifically to when law enforcement can use this technique in public DNA databases.

As previously stated, warrants are needed for almost every search and they are only provided when the investigator has shown probable cause. Therefore, genetic databases, even though they are digital, should be treated the same as any physical search of a home or building;

a warrant must be obtained in order to search online public genetic databases. This would ensure that various innocent people are not implicated and affected by investigations. Although the police can use databases to identify potential suspects, they must use traditional investigative techniques to narrow down the suspect pool prior to searching a database. One possible solution to still allow law enforcement access to public genetic databases would be put restrictions on when they can be used. Several states have already enacted criteria for these searches in state databases, including that the crime must be serious and that traditional methods have been exhausted without success (Ram et al. 5).

With regard to the constitutional aspect of the relationship between the Fourth Amendment and privacy, it is necessary to combine both aspects discussed earlier: digital and DNA. In *Maryland v King*, the Court ruled that DNA swabs were constitutional specifically for individuals arrested on felony charges. In *US v Jones*, GPS tracking in violation of a warrant was ruled unconstitutional. Cell phone access was ruled unconstitutional in both *Riley v US* and *Carpenter v US*. *Katz v US* emphasized the idea of a "reasonable expectation of privacy." From this small selection of cases, the Court appears to side with the individual when it comes to technological privacy. Ideally, they would continue to do the same if they were ever asked to hear a case relating to law enforcement's use of online public genetic databases. The privacy of the individual is crucial, especially with regard to genetic databases because people should be able to go about their lives without being constantly concerned about being investigated for a crime they never committed. It is a slippery slope to use new, unregulated technologies that potentially infringe on an individual's constitutionally guaranteed privacy.

Conclusion

Even if one feels the question of what to do about partial familial searches using public ancestry databases is not an issue of privacy, it poses a concern for democratic accountability ("Fortuity…" 789). Currently in America, many states have policies about this topic that are not accessible to the public; instead they are tucked away in lab manuals, accessible only to lab technicians (Ibid 776). If the public is unable to read the policies and become knowledgeable of what is in them, they cannot ensure that proper procedures and regulations are appropriately carried out.

One of the fundamental traits of a good democracy is the willingness of its people to question and scrutinize issues every time anything new happens; this goes for policies, techniques, and decisions. This characteristic functions in part to allow citizens to determine whether or not the new idea will threaten or infringe on their rights in a way that is unacceptable. With regard to the question at hand, America has the chance to decide. Although some states have regulations pertaining to searches within state databases, laws do not yet apply to public genealogy websites. There are no Supreme Court decisions regarding this question and very little scholarly writing about it. Now is the time for America to question, analyze, and dissect every miniscule aspect of this technique, before the Court determines what is going to happen. To borrow from the main principle established in *Katz v US*, it is the duty and responsibility of Americans to decide whether or not there is a socially acknowledged, reasonable expectation to privacy when using and uploading information onto public ancestry databases.

Works Cited

Aronson, Jay D.. *Genetic Witness: Science, Law, and Controversy in the Making of DNA Profiling*, Rutgers University Press, 2007.

"Bill of Rights." *Bill of Rights Institute*, billofrightsinstitute.org/founding-documents/bill-of-rights/.

Brown, Bruce. "DNA link to Golden State Killer raises questions of privacy versus safety." *Fox News*, 30 Apr. 2018.

California v Greenwood. 486 US 35 (1988). United States Supreme Court. 2018. Print.

Carpenter v United States. 585 US __ (2018). United States Supreme Court. 2018. Print.

Easteal, Simon, Neil McLeod, and Ken Reed. *DNA Profiling: Principles, Pitfalls, and Potential*. Harwood Academic Publishers: Langhorne, PA, 1993.

Fortin, Jacey. *In Serial Rape Case That Stumped Police, Genealogy Database Leads to Arrest*. The New York Times, 23 Aug. 2018, www.nytimes.com/2018/08/23/us/ramsey-street-rapist-dna.html.

Griswold v Connecticut. 381 US 479 (1965). United States Supreme Court. 1965. https://supreme.justia.com/cases/federal/us/381/479/#tab-opinion-1945663.

Hasian Jr, Marouf. "Vernacular Legal Discourse: Revisiting the Public Acceptance of the ''Right to Privacy'' in the 1960s." Political Communication, vol. 18, no. 1, Jan. 2001, pp. 89–105. EBSCOhost, doi:10.1080/10584600150217677.

Henry, Patrick. "Speech at Virginia Ratifying Convention, June 24, 1788." *Constitution Society*, www.constitution.org/rc/rat_va_20.htm.

Kase, Elizabeth S., et al. “Does the Warrantless Utilization of DNA Against a Non-Consenting Third Party Violate the Fourth Amendment.” Nassau Lawyer, Nov. 2018, pp. 8–26., www.abramslaw.com/webfiles/pdfs/2018111583642_000.pdf.

Katz v United States. 389 US 347. 347-374. United States Supreme Court. Print. 1967.

Kaye, David. “Why so Contrived? Fourth Amendment Balancing, Per se rules, and DNA Databases after Maryland v King.” *Journal of Criminal Law and Criminology*, 104, 3, 2014, 535-595.

Khamooshi, Arash. “Breaking Down Apple's IPhone Fight with the U.S. Government.” *New York Times*, 21 Mar. 2016.

Krimsky, Sheldon and Tania Simoncelli. *Genetic Justice: DNA Data Banks, Criminal Investigations, and Civil Liberties*, Columbia University Press, 2011.

Kyllo v United States. 533 US 27 (2001). United States Supreme Court. Print. 2001.

Lussenhop, Jessica. “Golden State Killer: The end of a 40-year hunt?” *BBC News*, 29 April 2018.

Maryland v King. 569 US 435. United States Supreme Court. Print. 2013.

Mustian, Jim. “New Orleans Filmmaker Cleared in Cold-Case Murder; False Positive Highlights Limitations of Familial DNA Searches.” *The Advocate*, 12 Mar. 2015, www.theadvocate.com/new_orleans/news/article_1b3a3f96-d574-59e0-9c6a-c3c7c0d2f166.html.

Olmstead v United States. 277 US 438. 437-488. United States Supreme Court. 1927. Print.

“Proposition 69.” *California Department of Justice.* https://oag.ca.gov/bfs/prop69.

Ram, Natalie. “DNA by the Entirety.” *Columbia Law Review*, vol. 115, 2015, papers.ssrn.com/sol3/papers.cfm?abstract_id=2645986.

Ram, Natalie. "Fortuity and Forensic Familial Identification." *Stanford Law Review*, vol. 63, 2011, papers.ssrn.com/sol3/papers.cfm?abstract_id=2298286.

Ram, Natalie, et al. "Genealogy Databases and the Future of Criminal Investigation." *Science*, vol. 360, no. 6393, 8 June 2018, doi:10.1126/science.aau1083.

Riley v California. 573 US __ (2014). United States Supreme Court. Print. 2014.

Roewer, Lutz. "DNA Fingerprinting in Forensics: Past, Present, Future." *Investigative Genetics*, 4(22), 2013. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3831584/.

"Senate Committee Findings on Illegal Intelligence Activities." *The Annals of America*, vol. 20, Encyclopaedia Britannica, Inc., 1976 pp. 276-284.

United States v Jones. 565 US ___ (2012). United States Supreme Court. Print. 2012.

United States v Miller. 425 US 435. United States Supreme Court. 1976. https://supreme.justia.com/cases/federal/us/425/435/.

Woods, Danielle. "Same Genetics Company Used in Golden State Killer and Christy Mirack Investigations." *WGAL*, Hearst Television, 26 June 2018, www.wgal.com/article/same-genetics-company-used-in-golden-state-killer-and-christy-mirack-investigations/21940947.