Familial DNA and the Fourth Amendment

Caden Chamma

Police have used data banks with the offender's DNA for years to compare samples with those found at crime scenes. Law enforcement agencies have now added another source: familial DNA databases used by the public that help search for relatives. The problem arises in the legality of using familial DNA. If the sample of one's DNA is taken legally with the suspect's permission, or a warrant was legally obtained to get the sample of DNA, then there is no issue. However, if the sample is taken without the knowledge of oneself, at what point can that DNA be used to solve a crime and incriminate someone? The process of solving crimes using your DNA has raised privacy and ethical concerns. Additionally, there is controversy surrounding whether the Fourth Amendment protects your rights against the use of DNA. The Fourth Amendment protects people from unreasonable searches and seizures by the government. The Fourth Amendment, however, is not a guarantee against all searches and seizures, but only those that are deemed unreasonable under the law (What Does the Fourth Amendment Mean). One of the current issues is whether the police can obtain DNA information through search and seizure using familial DNA. Sites like "My Family Tree," "23andMe" and "Ancestry" have been at the top of this discussion. Using one's family tree to solve crimes without consent has brought on a debate of whether Fourth Amendment rights are being violated. It is my view that once your information is given to a third party you should have no expectation of privacy and therefore your Fourth Amendment rights are not being violated. Not only will I discuss the familial database process, I will address the ethical and privacy concerns of using familial DNA in these databanks to help law enforcement solve crime. I will also discuss whether the Fourth Amendment applies to protect the privacy of one's DNA without consent. Furthermore, I will show the importance of familial DNA and how these genealogy sites are crucial for law enforcement to solve crime. Though the familial DNA databases are widely used by the public, the scope of the law for these databases should be widened. Law enforcement should have unconditional access to familial databases for solving crimes.

Over the last 40 years, the process of DNA has evolved to almost an exact science. A miniscule sample of DNA left at a crime scene can help solve any case. The comparison of DNA evidence can help establish if the sample matches a suspect to a crime. Each strand of DNA from an individual contains unique genetic information that only applies to that person. DNA samples can be used for comparison in a database that might already be formed, called a databank, to help analyze a sample of DNA that is provided by a criminal suspect. Technology advancements to DNA have made the storing of one's DNA profile, which can be based on hair or bodily fluid samples, more efficient. These samples are stored in a database to help search for suspects in current and cold cases. The National Offender Index compares crime scene samples against the database of profiles kept on file to help convict or exonerate individuals charged with crimes. The advances made by tracing DNA to identify criminal suspects has helped remodel the prosecution of criminals. "Advances in forensic science over the last decade are revolutionizing the possibilities of criminal investigation. In particular, the once controversial use of DNA

analyses to link previously identified suspects to crimes is being supplemented by large databases of the DNA types of convicted offenders or arrestees" (Lindsey 147). For example, the main database that law enforcement agencies use for DNA around the nation is the Combined DNA Index System. Adding familial DNA databases to existing databases extends the possibility of expanded searches.

The genetics of one's family history is readily available for use through the technology and advancement of DNA testing. Family DNA history databases are used to track family and genetic history, supply information about siblings, and help provide a link to family members that might not otherwise be available. In hopes of connecting with long lost relatives, people supply DNA swabs to these companies. Exploring one's ancestry has become increasingly popular over the years. However, the data provided by the DNA samples continue to build a massive database to help police solve crimes that have forensic DNA samples to compare with. Private companies that gather this information have changed the game of crime solving by expanding the data pool of family members and their family tree. The family tree forms a type of puzzle that branches out in different directions with extended family members. As more information is gathered, the bigger the family tree becomes. When family history databases began, there were no systems in place for the familial information given, and it was unprotected. Police were using the genetic markers of familial DNA to help narrow down suspects in their crime cases. Police use the puzzles that are created to form their own list of suspects and work down the family tree to eliminate potential suspects. As they exclude suspects from the family tree, they can narrow down the list of potential suspects to investigate. This includes not only current cases, but also brings cold cases to the forefront of investigation through the use of DNA.

One of the biggest crime cases to be solved through DNA testing using a genetic genealogy website is that of the "The Golden State Killer." Joseph James DeAngelo, otherwise known as the Golden State Killer, is responsible for at least 50 rapes, 120 burglaries, and 13 murders across California between 1973 and 1986. When DeAngelo was arrested in 2018, prosecutors confirmed he was caught using family tree searches on genealogy websites that helped narrow down close relatives to the DNA evidence matched at the crime scene (St. John). The ability to use these websites helped find a DNA match that identified and linked the killer to the crime scenes. How the police solved the crime using the Familial DNA has brought attention to the process of using these websites. First, they sent material from a genetic rape kit to FamilyTreeDNA, and that allowed a falsified account to set up future matching samples that might spark a lead. Then, when that produced a possible lead, they sent the profile to another website, MyHeritage (St. John). It was that search that helped identify a close relative to the original sample. With help from the close relative's family history, it narrowed down the suspect to one person, Joseph James DeAngelo. A match from a discarded tissue matched the DNA at crime scenes. Although his arrest sparked debates about using these websites, DeAngelo was convicted and sentenced to 26 life sentences (St. John).

Another case that demonstrates the value of using familial DNA is the cold case of Michelle Martinko. This case was solved by forming a family tree after getting a DNA hit. It was a 40-year-old murder that was solved with the help of familial DNA. Michelle Martinko was 18 at the time of her disappearance. With no leads, the case went cold for 40 years until the crime

scene DNA was uploaded to GEDmatch, and a hit from a distant relative showed a close match (Yuccas). It was then the police put together a family tree of a distant relative. Police narrowed it down to three brothers and followed each one until they left something behind to test for DNA. The DNA of one of the brothers, was collected off a straw left behind after leaving a restaurant (Yuccas). After DNA analysis, it was a confirmed match to evidence left at the crime scene. In August of 2020, Jerry Burns was convicted of the 1979 murder of Michelle Martinko (Yuccas). Like that of the Golden State Killer, this case also raised ethical concerns but was allowed to proceed in court.

Two of the biggest companies that provided information about the Golden State Killer denied any connection to their websites, absolving them of any responsibility for the sharing of information. After the controversy of using familial DNA websites to convict the Golden State Killer, genealogy companies rushed to ensure the public that their privacy was protected. 23andME promised to protect user privacy and issued the following statement. "It's our policy to resist law enforcement inquires to protect customer privacy" (Ram 1406). After the Golden State Killer case, the Department of Justice released a new rule that police cannot upload a fake profile to these websites to bypass rules set in place. Police must be transparent in their searches of these websites in order to use any information that might be provided to them. In an effort to protect one's privacy, the Department of Justice intended to balance public safety and privacy with their commitment to solve crimes of violent offenders. The issue with this law is that the policy states that police can use the database if the genealogy website permits it, and the police just need to be transparent in their searches. Being that there are so many loopholes in the law regarding the Fourth Amendment, genetic genealogy websites have taken it upon themselves to tighten up their privacy policies. In 2019, most genealogy companies created an "opt-in" policy that requires the consumer to agree that the DNA provided can be used by law enforcement. Due to this policy alone, the data search availability has been reduced by 90 % of what profiles that can be searched. The data provided dropped from about 1.4 million samples to roughly 140,000 samples after the opt in policy (Kaiser). Even though the opt-in policy is clearly stated, most third-party genealogy websites readily admit that DNA samples are shared with law enforcement under the assumption that the search has reasonable cause.

Besides the controversy of privacy, there is an ethical issue as well for these companies to stay transparent for what information is to be shared. "'The ethical challenge is how to balance public protection with individual rights,' says Malia Fullerton, D.Phil., an associate professor of bioethics and humanities at the University of Washington School of Medicine" (Princing). This balance is what brings the Fourth Amendment rights into consideration with DNA, but there are also other concerns. "Should police be able to so easily access databases? Most people say yes, especially in cases of violent crime. But where does privacy get to be overridden?' There are no clear answers, and opinions vary. But one important thing, Fullerton says, is transparency" (Princing). Transparency is important in terms of ethics as it holds law enforcement agencies to a work standard. Ethics help one from determining what might be considered right or wrong before taking an action. Law is decided by the government to protect its citizens from issues that might arise. The two should not be confused. Just because something might not be deemed ethical by some does not mean that it is against the law that was made to protect them. Although

there is controversy on both sides of the issue of whether ethics and transparency should play a part in determining the law, the law should only be decided on how it is written without considering any outside factors.

The interpretation of the Fourth Amendment varies among people, but the wording is crucial to how it is interpreted within the law. As I stated in the introduction, the Fourth Amendment prohibits unreasonable searches and seizures by the government. The Fourth Amendment, however, is not a guarantee against all searches and seizures, but only those that are deemed unreasonable under the law (What Does the Fourth Amendment Mean). One of the main problems is what classifies as an unreasonable search. At what point does a search stretch the boundaries of the law? The definition of what is classified as reasonable leaves many loopholes in the law. "The Supreme Court has carved out numerous exceptions to those requirements, finely granulating when searches are reasonable without a warrant or probable cause in some fact patterns, and at other times leaving outcomes dependent upon an amorphous balancing test … when 'the government violates a subjective expectation of privacy that society recognizes as reasonable" (Kimel 941). The issue with using the Fourth Amendment rights to protect one from using DNA based off familial websites is based on what is reasonable. Due to numerous exemptions made by the Supreme Court, there are ways to bypass the legitimacy of one's use of the Fourth Amendment. If it is declared a reasonable search, then all information collected is available to analyze. Right now, many could make an argument that it is unconstitutional to use this DNA. Several scenarios suggest that law enforcement agencies could catch more criminals but be a prisoner to our own government system with their overuse of loopholes in the wording. As of now, the law states that if someone would give their DNA to a third party, then they should have not had any expectation that their information would remain confidential. "Suspects who convey information to a third party, even if only incidentally, lose their rights to have it treated as private, and so the police may gain access to it without probable cause or even reasonable suspicion." (Stern 365). This shows how some information is already public domain, and if information is public, it avoids protection from the Fourth Amendment and is open to all. The issue with familial DNA is still in the courts regarding which searches are lawful and the violation of someone's rights regarding the protection by the Fourth Amendment. Even then, there are loopholes available for search and seizures by the police and government agencies. Regulations and legislation have not caught up with the loopholes in using these sites.

The way the law is written and understood states that if one voluntarily gives their information to a third party, they should not have any expectations of privacy; therefore, they are not protected under the Fourth Amendment. "In previous challenges to forensic DNA identification, courts have ruled against claims that it involves unreasonable searches and seizures prohibited by the Fourth Amendment" (Dresser 12). Until these challenges do not favor law enforcement, information collected in these databases should be readily available to analyze. When it comes to genealogy companies, the law is blurred in how their databases should be utilized. The law has established that police must be transparent with their searches and not use fake profiles like they did in the Golden State Killer case. Additionally, these private companies have their own rules. However, police and law enforcement agencies should be able to bypass them because they are afforded reasonable search and seizures. Without restrictions of familial

DNA databases, violent offenders that are a danger to communities can be imprisoned more efficiently. Limitless restrictions on familial DNA databases can raise questions of ethical concerns. One of these ethical concerns is privacy. If one has committed a crime that goes against the law, then why should the same law protect their privacy? At the same time, ethics and the law are in two different spheres. Ethics is based on someone's opinions of what they think is morally right or wrong. Ethics is not part of the law. Laws are written rules that are enforced unlike ethics, which are views based on standards or opinions. Decisions should be based on the way the law is written, not by interpretation. When determining Fourth Amendment issues in court, the decision comes down to reasonable searches and seizures. In terms of DNA, there are not defined laws on how to obtain and analyze DNA samples. DNA evidence is one of the strongest types of evidence to show in court as it is individual and precise. To hold an agency back because of ethics and not the law would limit the capabilities of solving crimes. Until the law changes and specifically details how to access DNA data in these databases, law enforcement agencies should have unconditional access to these sites to solve crimes. What might not be seen as ethical is still lawful.

Ethics and transparency should not be considered when defining the law. The law should be based on solely how it is written. What some might find unethical clearly does not mean it is protected by the law. The Fourth Amendment does not apply protection against the use of DNA to solve crimes as there is some degree of public access. Until the law is more transparent on the acquisition of DNA, the law cannot protect DNA as it is not completely private information. One should not have any expectation of privacy when supplying a third party with DNA. If DNA databases are used at their full potential, many violent crimes will be solved or possibly even prevented with the identification process that these data banks provide. Law enforcement should have unrestricted access to familial DNA databases.

Works Cited

Dresser, Rebecca. "At Law: Families and Forensic DNA Profiles." *The Hastings Center Report*, vol. 41, no. 3, 2011, pp. 11–12.

Kaiser, Jocelyn. "New Federal Rules Limit Police Searches of Family Tree DNA Databases." *Science*, AAAS, 25 Sept. 2019.

Kimel, Catherine W. "DNA PROFILES, COMPUTER SEARCHES, AND THE FOURTH AMENDMENT." *Duke Law Journal*, vol. 62, no. 4, 2013, pp. 933–973.

Lindsey, Samuel, et al. "COMMUNICATING STATISTICAL DNA EVIDENCE." *Jurimetrics*, vol. 43, no. 2, 2003, pp. 147–163.

Princing, McKenna. "Will Your Genealogy Help Solve a Murder – or Get You Accused of One?" *Right as Rain by UW Medicine*, UW Medicine, 10 Jan. 2019.

Ram, Natalie. "GENETIC PRIVACY AFTER *CARPENTER*." *Virginia Law Review*, vol. 105, no. 7, 2019, pp. 1357–1425.

Stern, Simon. "The Third-Party Doctrine and the Third Person." *New Criminal Law Review: An International and Interdisciplinary Journal*, vol. 16, no. 3, 2013, pp. 364–412.

St. John, Paige. *The Untold Story of How the Golden State Killer Was Found: A Covert Operation and Private DNA*. 8 Dec. 2020, www.latimes.com/california/story/2020-12-08/man-in-the-window.

"What Does the Fourth Amendment Mean?" *United States Courts*, www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0.

Yuccas, Jamie. "Young Murder Victim Helps Solve Her Own Cold Case Nearly 40 Years Later." *CBS News*, CBS Interactive, 7 Nov. 2020, www.cbsnews.com/news/michelle-martinko-murder-victim-solve-cold-case-40-years-later/.