Journal of Civil Rights and Economic Development

Volume 34
Issue 3 *Volume 34, Summer 2021, Issue 3*

Article 5

Solving Crimes with 23andMe: DNA Databases and the Future of Law Enforcement

Meghan McLoughlin

SOLVING CRIMES WITH 23ANDME: DNA DATABASES AND THE FUTURE OF LAW ENFORCEMENT

MEGHAN MCLOUGHLIN

INTRODUCTION

"It could never happen to me though, right?"

Sitting on our comfortable couches in our secure homes and watching news stories about people who have lost loved ones to the most terrible, violent crimes, we think to ourselves: "That's awful for them, but it won't happen to me." But what if it did?

Becoming a victim of a violent crime or loving someone who becomes a victim of a crime in the United States is not uncommon. In 2016, 2.9 million people in the United States were victims of at least one "violent crime"—crimes defined by their inherent violence, which include offenses like rape, murder, and sexual assault.[1] In the same year, 28.4% of people between the ages of twenty-five and thirty-four were victims of violent crimes—for females, that percentage grew to 33.4%.[2] In fact, the United States has been reported to be one of the most dangerous countries in the world.[3]

[1] *See* Rachel E. Morgan & Grace Kena, *Criminal Victimization 2016: Revised*, BUREAU OF JUST. STAT. (Oct. 2018), https://www.bjs.gov/content/pub/pdf/cv16re.pdf (clarifying that "[v]iolent crime includes murder, rape and sexual assault, robbery, and assault."). In most states, rape differs from sexual assault because it requires penetration; sexual assault can consist of any sort of unwanted sexual touching. *See An Updated Definition of Rape*, U.S DEPT. OF JUST. ARCHIVES (Jan. 6, 2012), https://www.justice.gov/archives/opa/blog/updated-definition-rap; *see also Sexual Assault*, RAINN, https://www.rainn.org/articles/sexual-assault (last visited Feb. 10, 2021).

[2] *See* Morgan & Kena, *supra* note 1. And those numbers are not changing any time soon—the United States Department of Justice reported that there was no statistically significant change in those numbers from the data collected in 2015. *See id.*

[3] *See* Laura Begley Bloom, *Revealed: The 15 Most Dangerous Places to Live,* FORBES (Sept. 27, 2018), https://www.forbes.com/sites/laurabegleybloom/2018/09/27/revealed-the-15-most-dangerous-places-to-live/#729eb19f4706. In this survey, 18,135 ex-pats living in 187 territories outside the US ranked the territories based on peacefulness, personal safety,

Even worse, many of these crimes go unsolved. In the past decade, 54,868 homicides were committed in the United States.[4] Out of those, *fifty percent* never resulted in an arrest of any suspect.[5] In 2017, only 34.5% of reported rapes resulted in the prosecution or identification of any perpetrator.[6] Violent crimes are uniquely situated because perpetrators often leave behind DNA at the crime scenes—but even if a full forensic DNA profile was able to be salvaged, too often the forensic sample does not match any profile in the DNA databases of the criminal justice system.[7] This situation creates a dead-end for law enforcement: no arrest can be made since a forensic profile with no match in the system is like finding a fingerprint without a suspect's name attached to it—it is just a useless, anonymous profile.[8]

So, what if there was a way for law enforcement to increase its ability to solve these violent crimes? What if law enforcement could theoretically access millions[9] of more DNA profiles to compare to their "John Doe" profiles,[10] thereby solving violent crimes that haven't been solved in decades? What if solace could finally be given to those victims and their families, and what if violent criminals could be prevented from committing these vicious crimes for years on end?

Law enforcement has indeed found a way. In 2018, for the first time, police sought to broaden their number of DNA profile comparisons to more than just the profiles in the criminal justice system's database.[11] They did so for one particular suspect, dubbed

and political stability—the United States was ranked at just 67% positive in personal safety, which is 15% lower than the global average. *See id.*

4 *See* Steven Rich et al., *Murder with Impunity*, WASH. POST, https://www.washingtonpost.com/graphics/2018/investigations/unsolved-homicide-database/?utm_term=.c939ebf721ca (last updated July 6, 2018).

5 *See id.*

6 *See Clearances*, FBI: UCR (2017), https://ucr.fbi.gov/crime-in-the-u.s/2017/crime-in-the-u.s.-2017/topic-pages/clearances.

7 *See Using DNA to Solve Crimes*, U.S. DEPT. OF JUST. ARCHIVES, https://www.justice.gov/archives/ag/advancing-justice-through-dna-technology-using-dna-solve-crimes.

8 *See* Eric Levenson*, It Started as a Hobby. Now They're Using DNA to Help Cops Crack Cold Cases*, CNN (March 27, 2019), https://www.cnn.com/2018/08/03/health/dna-genealogy-cold-cases-trnd/index.html.

9 *Ancestry Surpasses 5 Million People in DNA Database, Giving Customers Even More Opportunities to Discover Who They Are and How They Connect to One Another*, ANCESTRYDNA (Aug. 9, 2017), https://www.ancestry.com/corporate/newsroom/press-releases/ancestry-surpasses-5-million-people-dna-database-giving-customers-even-more.

10 "John Doe" profiles are what law enforcement call forensic profiles for which there is no identifying match in their system.

11 *See* Sam Stanton & Darrell Smith, *How Detectives Collected DNA Samples From the*

"The Golden State Killer," who had committed at least sixty murders and rapes that had gone unsolved in California for over forty years.[12] Instead of only submitting the forensic profile found at the scene to the national law enforcement database, as they had done many times to no avail, law enforcement thought of a new way to find a match. This time, detectives submitted the forensic profile to GEDMatch.[13]

GEDMatch is a genealogy service that allows a customer to submit his genetic information that has already been analyzed by a laboratory in order to compare that genetic information against the GEDMatch database and potentially find unknown relatives and other genealogy facts.[14] Using this website, law enforcement *did* get a hit—not on the suspect, but on one of his relatives.[15] According to GEDMatch, someone genetically related to the suspect had previously submitted his DNA information to the website for comparison purposes; the relative's DNA sample remained in the database and was thus genetically linked to the profile submitted by the law enforcement officers.[16] Now possessing the name of this relative, police were able to narrow down their large suspect pool to only those people who were in the area at the time of the crimes *and* were also related to this relative found on GEDMatch.[17] After a lengthy investigation into the branches of this relative's family tree, the only suspect that satisfied all of law enforcement's criteria was a man named Joseph DeAngelo.[18] Using this information, the police were able to obtain a surreptitious[19] sample of Joseph DeAngelo's DNA to compare to the samples found at the crime

East Area Rapist Suspect, SACRAMENTO BEE (June 1, 2018, 4:35 PM), https://www.sacbee.com/latest-news/article212334279.html.

12 *See id.*

13 *See* Avi Selk, *The Ingenious and 'Dystopian' DNA Technique Police Used to Hunt the 'Golden State Killer' Suspect*, WASH. POST (April 28, 2018, 1:50 PM), *https://www.washingtonpost.com/news/true-crime/wp/2018/04/27/golden-state-killer-dna-website-gedmatch-was-used-to-identify-joseph-deangelo-as-suspect-police-say/*

14 *See GEDmatch.Com Terms of Service and Privacy Policy,* GEDMATCH, https://www.gedmatch.com/tos.htm (last updated Dec. 9, 2019) [hereinafter GEDmatch].

15 *See* Stanton & Smith, *supra* note 11.

16 *See* Selk, *supra* note 13.

17 *See id.*

18 *See id.*

19 *See* Paige St. John & Joseph Serna, *Golden State Killer Suspect Must Provide New DNA Samples and Fingerprints, Judge Rules,* LA TIMES, (May 3, 2018, 9:20 AM), https://www.latimes.com/local/lanow/la-me-ln-golden-state-killer-evidence-20180503-story.html. Law enforcement uses "surreptitious sample" to refer to those DNA samples collected without the knowledge of the suspect. *See id.*

scenes—which was a match—and finally arrested him for the rapes and murders he allegedly committed over forty years ago.[20]

Commercial DNA databases from genealogy companies could give law enforcement access to over fifteen-million more profiles to compare against a suspect's sample—that's fifteen-million more chances to catch the killer of a loved one and to prevent him from hurting anyone again.[21] A recent study shows that it would take just two percent of the adult population's DNA to be able to connect virtually anyone in the world to another—meaning that law enforcement would be able to narrow down almost every suspect pool once they gathered a DNA profile from a crime scene.[22] Rockne Harmon, a former senior deputy district attorney in California, insists that if familial testing was more widely used, law enforcement "would solve twice as many cases as [they] do now."[23] Moreover, granting law enforcement access to these databases could even *prevent* crime by way of deterrence—lowering violent criminals' likelihood of reoffending by as much as seventeen percent.[24] If this method had existed in the 1970s, it is likely that the Golden State Killer would not have had the opportunity to commit all the crimes he did.

However, immediately after this technological breakthrough, questions arose as to whether the method could be considered a constitutional search under the Fourth Amendment. While proponents of law enforcement welcomed the new technology, others admonished the method as a violation of commercial database customers' privacy rights, fearing the implications of this massive tool for law enforcement.[25] Many news outlets and commentators have

---

[20] *See id.*

[21] *See* Lindsey Van Ness, *DNA Databases Are Boon to Police But Menace to Privacy, Critics Say*, PEW (Feb. 20, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/20/dna-databases-are-boon-to-police-but-menace-to-privacy-critics-say.

[22] *See* Yaniv Erlich et al., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCIENCE 690, 690–694 (2018), https://science.sciencemag.org/content/362/6415/690.

[23] James Rainey, *Familial DNA Puts Elusive Killers Behind Bars. But Only 12 States Use It.*, NBC NEWS (April 28, 2018, 6:00 AM), https://www.nbcnews.com/news/us-news/familial-dna-puts-elusive-killers-behind-bars-only-12-states-n869711.

[24] *See* Jennifer Doleac, *Can DNA Databases Reduce Crime Rates?*, FORBES (May 16, 2017, 3:49 PM), https://www.forbes.com/sites/quora/2017/05/16/can-dna-databases-reduce-crime-rates/#391929805712.

[25] *See* Matt Ford, *How the Supreme Court Could Rewrite the Rules for DNA Searches*, NEW REPUBLIC (Apr. 30, 2018), https://newrepublic.com/article/148170/supreme-court-rewrite-rules-dna-searches.

even started warning people not to submit DNA to these companies.[26]

Since the Golden State Killer case, some large commercial DNA databases have already started holding press conferences pledging to never cooperate with law enforcement unless they are forced.[27] Advocates have called for courts to declare the unconstitutionality of these searches and to bar law enforcement's use of these databases altogether.[28] In fact, one state has even proposed a bill barring law enforcement from accessing these databases for crime-solving purposes altogether, claiming that the use by law enforcement violates the Fourth Amendment.[29]

This note rejects these objections and petitions for change as wrongheaded. Law enforcement access to commercial DNA databases is constitutional under the Fourth Amendment because the government's interest in public safety outweighs the small expectation of privacy in samples of DNA voluntarily given to a third party, particularly when used to prevent violent or sexual assault crimes. Specifically, this access is constitutional under the third-party doctrine of the Fourth Amendment.

Part I of this note provides background through the discussion of two topics: first, the history of DNA evidence in law enforcement leading up to the use of commercial DNA databases; and second, the concerns of privacy advocates that threaten the use of this search method by law enforcement. Part II of this note explains

---

26 CTVNews.ca Staff, *Privacy expert warns of risks of submitting DNA to genealogy websites*, CTV NEWS (Apr. 25, 2018, 10:23 AM), https://www.ctvnews.ca/sci-tech/privacy-expert-warns-of-risks-of-submitting-dna-to-genealogy-websites-1.3901264.

27 *See generally Ancestry Guide for Law Enforcement*, ANCESTRYDNA, https://www.ancestry.com/cs/legal/lawenforcement (last visited Feb. 12, 2021) [hereinafter Ancestry Law Enforcement Guide]; *see generally also 23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide (last visited Feb. 12, 2021) [23andMe Law Enforcement Guide]. It is important to note that this note does not discuss the analysis as to whether law enforcement can subpoena these companies into cooperating with law enforcement in these matters. This note simply discusses whether or not it is *constitutional* for law enforcement to use their services. However, the fact that the companies pledged to their customers not to cooperate is evidence of customer disapproval of law enforcement's use, shedding light on the fact that this view could be translated into law at some point.

28 Bloomberg, *DNA Detectives are Searching for Killers in Your Family Tree*, FORTUNE (June 14, 2018, 10:02 AM), http://fortune.com/2018/06/14/dna-genealogy-websites-police.

29 *See generally* Public Safety – DNA Analysis – Search of Data Base, H.B. 30, Reg. Sess. (Md. 2019); *see also* Natalie Jones, *Maryland House bill seeks to prohibit using familial DNA databases to solve crime*, BALTIMORE SUN (Feb. 20, 2019, 10:29 PM), https://www.baltimoresun.com/politics/bs-md-maryland-house-bill-dna-databases-0221-story.html.

the applicable law that will be used in the analysis: the third-party doctrine of the Fourth Amendment. Part III will explain exactly how this type of search is constitutional under the third-party doctrine of the Fourth Amendment by discussing the expectation of privacy implicated in this search as well as the high need by law enforcement to use this method of searching—which is a factor weighed in the analysis of whether a search is "reasonable" under the Fourth Amendment.[30]

I. BACKGROUND

A. DNA Usage

DNA evidence was first used by law enforcement in 1986 when police asked a molecular biologist to analyze the DNA of a seventeen-year-old boy who had confessed to the rapes and murders of two women in England.[31] However, the first conviction using DNA evidence was a rape case in California in 1987.[32] In that case, the DNA of the defendant, Tommy Lee Andrews, matched that of a semen sample left at the crime scene.[33] Since then, the use of DNA evidence in investigations has become commonplace[34] and even expected part of proving the identity of the person who committed a certain crime.[35]

30 *See* United States v. Miller, 425 U.S. 435, 5 (1976).

31 *See* Lisa Calandro et al., *Evolution of DNA Evidence for Crime Solving: A Judicial and Legislative History*, FORENSIC MAG (Jan. 6, 2005, 3:00 AM), https://www.forensicmag.com/article/2005/01/evolution-dna-evidence-crime-solving-judicial-and-legislative-history. In this case, the DNA was actually exculpatory—it proved the defendant was *not* the attacker. Eventually, that same DNA helped law enforcement find the true perpetrator. *Id.*

32 *See id.*

33 *See id.*

34 *See DNA Evidence in Criminal Cases,* NOLO, https://www.nolo.com/legal-encyclopedia/dna-evidence-its-genes-30060.html (last visited Feb. 12, 2021) "DNA testing is now common in criminal trials and in proving innocence after wrongful convictions." *Id.*

35 *See* Matthew Shaer, *The False Promise with DNA Testing*, THE ATLANTIC, 8-9, 35 (June 2016), https://www.theatlantic.com/magazine/archive/2016/06/a-reasonable-doubt/480747 "Three-quarters of the jurors said they expected DNA evidence in rape cases, and nearly half said they expected it in murder or attempted-murder cases; 22 percent said they expected DNA evidence in every criminal case." *Id.*

After the usefulness of DNA information was established, databases of DNA started forming. For the purposes of this note, there are two general types of DNA databases in existence today: governmental and commercial. The governmental DNA database is a bank of DNA profiles that have been collected for a government purpose.[36] When someone is convicted of a crime, his or her DNA is collected by the government.[37] In 2013, the Supreme Court held that it was constitutional to collect the DNA of people arrested for serious offenses and not exclusively convicted offenders.[38] Today, DNA samples in the governmental bank include those of missing persons, convicted offenders, arrestees, and unknown samples collected at the scene of a crime, known as forensic profiles.[39]

In the United States, the government's DNA databank is called the Combined DNA Index System (CODIS).[40] The database has several levels and was established in 1994 by the FBI.[41] The national level is referred to as the National DNA Index System (NDIS). In 2018, this database contained over 13.5 million convicted offender profiles, over three-million arrestee profiles, and almost one-million forensic profiles.[42] The inherent composition of this database is primarily made up of profiles of those individuals who have come in contact with the criminal justice system—as a victim *or* an offender—since the only profiles collected by the government are those that were involved in a crime in some form.[43]

Commercial DNA databases are comprised of an entirely different population. These databases, like AncestryDNA and 23andMe, are made up of DNA samples from people who affirmatively send in their DNA sample to the company for the purpose of

36 *See Federal DNA Database*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/federal-dna-database#:~:text=The%20Federal%20DNA%20Database%20Unit,by%20law%20to%20do%20so (last visited Feb. 12, 2021).

37 *See generally Frequently Asked Questions on CODIS and NDIS,* FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Feb. 12, 2021) [hereinafter NDIS Fact Sheet].

38 *See generally* Maryland v. King, 569 U.S. 435, 465-6 (2013).

39 *See generally CODIS-NDIS Statistics*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics (last visited Feb. 12, 2021) [hereinafter NDIS Statistics].

40 *See* NDIS Fact Sheet, *supra* note 37. The National DNA Index System or NDIS is considered one part of CODIS, the national level, containing the DNA profiles "contributed by federal, state, and local participating forensic laboratories." *Id.*

41 *See* Ford, *supra* note 25.

42 *See* NDIS Statistics, *supra* note 39.

43 *See* Ford, *supra* note 25.

obtaining a genealogical analysis of their DNA, irrespective of whether or not they have committed a crime in the past.[44] Most of these companies, referred to as "direct-to-consumer" genealogy service databases, send customers kits in which to deposit an actual DNA sample so that the company can analyze it in its own laboratory.[45] Created mostly after 2005,[46] these companies then analyze the sample, compare it against other samples in the databank, and send back results.[47] These databases, unlike the governmental database, are comprised of DNA samples from people who *voluntarily* submit their DNA to the company in order to receive a service.[48]

Still other commercial companies, like GEDMatch, simply compare a raw DNA profile submitted by a customer (that was already analyzed by a laboratory) to other raw data in its system without individually testing the sample in their own laboratories.[49] These companies do not ever possess any physical DNA samples. Instead, they receive the information a customer gives the company about his or her DNA and compare it against profile information that it has received from other customers.[50] Practically, these companies usually market their services as providing a secondary database to which people can submit the results that they receive from a commercial DNA database in order to compare their sample to another pool of peoples' information and obtain additional genealogical information.[51] These companies drastically expand the number of DNA profiles law enforcement can use for comparison

44 *See AncestryDNA- Frequently Asked Questions*, ANCESTRYDNA, https://www.ancestry.com/dna/en/legal/us/faq (last visited Jan. 30, 2021) [hereinafter AncestryDNA FAQ]; *see also How it works*, 23ANDME, https://mediacenter.23andme.com/howitworks (last visited Jan. 30, 2021) [hereinafter 23ANDME].

45 *See Ancestry Terms and Conditions*, ANCESTRYDNA (Sept. 23, 2020), https://www.ancestry.com/cs/legal/termsandconditions [hereinafter Ancestry DNA Terms]; *see also* 23ANDME, *supra* note 44.

46 *See Ancestry.com Launches New AncestryDNA Service: The Next Generation of DNA Science Poised to Enrich Family History Research,* ANCESTRYDNA, http://www.ancestry.com/corporate/newsroom/press-releases/ancestry.com-dna-launches (last visited Jan. 30, 2021); *see also About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us/ (last visited Jan. 30, 2021).

47 *See* AncestryDNA FAQ, *supra* note 44; *see also How Can I See The Status Of My DNA Sample?*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/202904780-How-Can-I-See-the-Status-of-My-DNA-Sample (last visited Jan. 30, 2021).

48 *See AncestryDNA Research Project*, ANCESTRYDNA, https://support.ancestry.com/s/article/AncestryDNA-Research-Project (last visited Jan. 30, 2021).

49 *See* GEDMatch, *supra* note 14.

50 *See id.*

51 *See id.*

since they are comprised of DNA results from a multitude of direct-to-consumer databases—making them almost more valuable than the original databases that actually analyze the results.[52]

Generally, governmental and commercial databases serve largely different purposes and are filled with different populations of people. As a result, the traditional method of searching these databases is different, because the searcher of one database is looking for different information than the searcher of another.

For instance, governmental databases are usually searched by submitting a certain profile to the database and conducting a search to find out if any DNA samples already in the database match that sample exactly—a method hereafter referred to as an "exact suspect search."[53] The purpose of this is to find out if the unknown owner of the submitted sample is already identified somewhere in the system because of a previous crime.[54]

Contrarily, commercial DNA databases are generally used for genealogical searches—hereafter referred to as a "familial search." Instead of looking for an exact match in the database when submitting a sample, the searcher is looking for samples from people who are part of the same family as the submitted sample.[55] Thus, instead of identification purposes, commercial databases are largely used for genealogical services, familial searching, and finding out more about the ancestry of the submitted sample.[56]

However, in recent years, law enforcement has tried incorporating familial searching into searches of the governmental databases.[57] Instead of just looking for an exact suspect match in a state's governmental database in order to identify the owner of a given DNA sample, a search would also be done to determine if any of the owner's family members could also be identified in the

---

52 *See* Bloomberg, *supra* note 28 ("In the case of DNA sites, no extraordinary measures may be necessary, as such services as GEDmatch, MyHeritage, and Family Tree DNA allow investigators to view voluntarily posted data, including files from services like 23andMe and Ancestry that don't permit users to upload material from other sources."). *See also* Levenson, *supra* note 8. AncestryDNA and 23andMe—two direct-to-consumer databases—consist of over 15 million DNA profiles for comparison alone. *See id.*

53 *See* NDIS Fact Sheet, *supra* note 37.

54 *See id.*

55 *See* AncestryDNA FAQ, *supra* note 44.

56 *See id.*; *see also* 23andMe Law Enforcement Guide*, supra* note 27.

57 *See* Sonia M. Suter, *All in the Family: Privacy and DNA Familial Searching*, 23 HARV. J. LAW & TEC 309, 310-11 (2010).

database.[58] Even though conducting a familial search would not provide law enforcement with the identity of the owner of the sample they submitted, it would give them a much narrower pool of possible owners.[59] A seminal case involving this technique took place in California in 2010, where police conducted a familial search in the national database with a sample found at the scene of a murder.[60] The perpetrator was not in the system, but his son was.[61] This result led the police to the perpetrator, a serial killer named Lonnie Franklin, Jr.[62]

This method of familial searching in the national database has been criticized by privacy rights advocates because it opens the door to a person being identified through a relative's DNA due to that relative committing a crime and thus having his DNA collected by the government.[63] As of April 2018, only twelve states, including California, had used any form of familial searching to solve cold cases.[64] Maryland and the District of Columbia banned the practice of conducting familial searches in their state databases altogether.[65]

Since then, law enforcement in California has taken this method even one step further. In April 2018, law enforcement used a *commercial* DNA database to identify family members of the DNA sample they recovered from the scene of a murder committed in the late 1970s.[66] The "East Area Rapist," later known as the "Golden State Killer,"[67] was an unidentified criminal who was

58 *See id.* at 311.

59 *See id.* at 318.

60 *See* Seth Augenstein, *Familial Searching, Used in 10 States and Counting, Solves the Unsolvable*, FORENSIC MAG (Dec. 8, 2016, 12:55 PM), https://www.forensicmag.com/news/2016/12/familial-searching-used-10-states-and-counting-solves-unsolvable.

61 *See id.*

62 *See id.*

63 *See* Suter, *supra* note 57, at 311-312.

64 *See* Rainey, *supra* note 23. Only Arizona, California, Colorado, Florida, Minnesota, New York, Ohio, Texas, Utah, Virginia, Wisconsin, and Wyoming had used any form of familial searching within their criminal DNA databases to solve crimes. *See id.*

65 *See id.* Since the DNA profiles obtained by law enforcement are usually not obtained from the person voluntarily (or by his own accord), the constitutionality of conducting a familial search of DNA profiles in the national database would undergo a separate Fourth Amendment analysis. *See* Suter, *supra* note 57, at 329. This separate analysis is outside the scope of this note.

66 *See* Selk, *supra* note 13.

67 *See* Laura Wamsley, *After Arrest of Suspected Golden State Killer, Details of His Life Emerge*, NPR (Apr. 26, 2018, 3:51 PM), https://www.npr.org/sections/thetwo-way/2018/04/26/606060349/after-arrest-of-suspected-golden-state-killer-details-of-his-life-

believed to have killed twelve people, raped at least fifty-one people, and burglarized countless California homes from 1974 through May 1986.[68] However, even though DNA evidence had been left at multiple scenes, law enforcement was never able to apprehend the killer because his DNA was not an exact match to any samples already in the FBI's national database.[69] That is until April 2018, over forty years later, when law enforcement used GEDMatch, a commercial DNA profile database, to identify family members of the forensic profile left at the scene.[70] In other words, instead of using law enforcement's own database, police searched a commercial database for genetic links to the forty-year-old unidentified forensic profile—and it worked. Law enforcement began searching "online family trees that appeared to match DNA samples from the East Area Rapist's crimes," and focused on those who lived in the area at the time of the crimes in order to determine a much more limited pool of possible suspects.[71]

Law enforcement was then able to narrow down suspects to Joseph DeAngelo, a person who was in the area during the commission of the crimes and was genetically linked to the forensic profile's family members.[72] Officers managed to collect a surreptitious DNA sample from him.[73] Then, when law enforcement ran DeAngelo's DNA sample against the forensic samples from the crime scenes, his sample was an exact match.[74] DeAngelo was then arrested for the various rapes and murders committed throughout the 1970s and 1980s.[75] Facing the death penalty, DeAngelo pled guilty to crimes he committed against eighty-seven victims spanning from 1975 to 1986 and was sentenced to eleven consecutive life terms without the possibility of parole.[76]

---

emerge. Joseph DeAngelo began his criminal career as a home-invasion rapist, but as time went on, he began killing his victims as well. Since his identity remained a mystery, his aliases changed to reflect the types of crimes he was committing. *See id.*

68 *See* Sam Stanton & Ryan Lillis, *Relative's DNA From Genealogy Websites Cracked East Area Rapist Case, DA's Office Says*, THE SACRAMENTO BEE (Apr. 26, 2018, 2:01 PM), https://www.sacbee.com/latest-news/article209913514.html.

69 *See* Selk, *supra* note 13.

70 *See id.*

71 Stanton & Lillis, *supra* note 68.

72 *See* Stanton & Smith, *supra* note 11.

73 *See id.*

74 *See* Stanton & Lillis, *supra* note 68.

75 *See* Stanton & Smith, *supra* note 11.

76 Michael Levenson, *Golden State Killer Sentenced to Life in Prison Without Parole*, NEW YORK TIMES (Aug. 21, 2020), https://www.nytimes.com/2020/08/21/us/golden-state-

After this breakthrough, California and other states began looking into using commercial DNA databases. In June 2018, Washington police were able to arrest the person they believed to have murdered twelve-year-old Michella Welch in 1986 using a genealogy service's commercial DNA database.[77] That same month, Pennsylvania law enforcement accessed a commercial DNA database to solve the murder of Christy Mirack, a school teacher, which happened in 1992.[78] In May, police in Indiana, using the same method, were able to locate a suspect for the 1988 rape and murder of April Tinsley, an eight-year-old girl.[79]

Most recently, evidence obtained through an investigation using a commercial DNA database was even presented in a trial for the first time.[80] On July 1, 2019, William Talbott II was convicted for a double homicide he committed in 1987.[81] Over thirty years after he murdered a couple in Washington, Talbott was arrested and tried in Snohomish County, where a jury found him guilty of two counts of aggravated first-degree murder.[82] That jury was the first ever to hear evidence that was collected using commercial DNA databases.[83]

Even still, questions are arising as to whether or not the use of commercial databases is a constitutional way to find suspects.[84] While supporters of law enforcement advocate for access to search tools, privacy rights enthusiasts criticize the intrusion.[85]

killer-sentenced.html.

77 *See* Levenson, *supra* note 8.

78 *See id.*

79 *See id.*

80 *See* Heather Murphy, *Genealogy Sites Have Helped Identify Suspects. Now They've Helped Convict One*, NEW YORK TIMES (July 1, 2019), https://www.nytimes.com/2019/07/01/us/dna-genetic-genealogy-trial.html.

81 *See id.; see also* Seattle Times Staff, *SeaTac Man Convicted of 1987 Murders of Canadian Couple after DNA Evidence Linked Him to Case*, THE SEATTLE TIMES (June 28, 2019, 3:58 PM), https://www.seattletimes.com/seattle-news/crime/seatac-man-convicted-of-1987-murders-of-canadian-couple-after-dna-evidence-linked-him-to-case/.

82 *See* Caleb Hutton, *Talbott trial testimony retraces a 30-year murder mystery*, HERALDNET (June 25, 2019, 12:24 PM), https://www.heraldnet.com/news/talbott-trial-testimony-retraces-a-30-year-murder-mystery; *see also* Seattle Times Staff, *supra* note 81.

83 *See* Murphy, *supra* note 80.

84 *See* Ford, *supra* note 25.

85 *See id.* "Handling such sensitive information creates additional challenges when it comes to balancing the individual right to privacy with the state's interest in combating crime." *Id.*

B. Privacy Concerns

Right around the time of the "Golden State Killer" case, privacy advocates began arguing that law enforcement's use of commercial DNA databases is essentially a "slippery slope" that implicates major privacy concerns.[86] Developments in science and technology have always been a challenge for courts and legislative bodies, as access to greater investigative power inevitably comes with it more risks implicating privacy rights.[87] In a recent study, privacy advocate Yaniv Erlich tested just how effective familial searches in commercial databases could be by submitting samples to get an idea of how many would lead to a familial match.[88] Erlich found that out of the samples he sent in, more than half had distant relatives who could be found in the commercial databases.[89] In fact, according to his research, "it will take only about two percent of an adult population having their DNA profiled in a database before it becomes theoretically possible to trace any person's distant relatives from a sample of unknown DNA—and therefore, to uncover their identity."[90] While some hail these results as promising for law enforcement, Erlich worried that with this amount of information came the risk of illegitimate uses, such as exploitation or use in medical studies without permission.[91] To combat this, some privacy advocates demand that law enforcement should only be able to access information from commercial databases by obtaining a warrant. But the warrant process as applied here, as discussed in later sections of this note, does not make sense.[92]

---

86 Ed Cara, *Ancestry Sites Could Soon Expose Nearly Anyone's Identity, Researchers Say*, GIZMODO (Oct 11, 2018, 2:37 PM), https://gizmodo.com/ancestry-sites-could-soon-expose-nearly-anyones-identit-1829685818 ". . .[D]own the road, as things continue to evolve, there could be people who use this for illegitimate reasons." *Id.*

87 *See e.g.*, Kyllo v. United States, 533 U.S. 27 (2001); *see also* Riley v. California, 573 U.S. 373 (2014).

88 *See* Erlich et al., *supra* note 22.

89 *See id.*

90 Cara, *supra* note 86. As of February 2019, more than 26 million people have taken an at-home ancestry test. This constitutes only about 0.35% of the world's population. *See* Antonio Regalado, *More than 26 million people have taken an at-home ancestry test*, MIT TECHNOLOGY REVIEW (Feb. 11, 2019), https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test.

91 *See id.*

92 *See id.* ("In an ideal world, law enforcement agencies could also still access these services, but only obtaining after explicit permission, such as through a warrant."); *see also infra*, note 190 and accompanying text.

Some call for new laws to prohibit law enforcement's use altogether.[93] Jennifer Lynch, a senior attorney at the Electric Frontier Foundation, noted that since genetic information has not been expressly protected under the Fourth Amendment, "[t]here are no meaningful protections. And we need them."[94] In addition, the American Civil Liberties Union's (ACLU) Vera Eidelman has made claims that law enforcement's use of the databases implicates illegality.[95] Eidelman remarked that because companies like 23andMe lack legally reliable evidence that a certain DNA sample or account is connected to a certain person, it should not be considered "proof in a legal context."[96]

Significantly, a Maryland legislator has even proposed a law[97] that would "prohibit use of a familial DNA database for the purposes of crime-solving."[98] The bill, sponsored by Delegate Charles Sydnor, seeks to ban law enforcement from accessing "popular consumer genetic databases" because the people submitting their DNA samples to the companies are doing so without the knowledge that law enforcement could access the information.[99] Sydnor claims that these types of searches are violations of the Fourth Amendment of the Constitution.[100] A journalist reported on the Talbott case stated: "The defense could have challenged the use of genetic genealogy on privacy grounds, or as a violation of people's right to control their personal data."[101]

Most recently, lawyers defending thirty-seven-year-old Jesse Bjerke in a Virginia rape case moved to suppress the DNA evidence inculpating the defendant that was first discovered using a commercial DNA database, arguing that "assembling and testing

93 *See* Bloomberg, *supra* note 28.

94 Bloomberg, *supra* note 28.

95 *See* Vera Eidelman, *Why the Golden State Killer Investigation is Cause for Concern,* ACLU (May 11, 2018), https://www.aclu.org/blog/privacy-technology/medical-and-genetic-privacy/why-golden-state-killer-investigation-cause.

96 *See id.*

97 *See* Public Safety – DNA Analysis – Search of Data Base, Md H.B. 30, Reg. Sess. (2019).

98 Natalie Jones, *Bill Seeks to Prohibit Using DNA Databases to Solve Crime*, AP NEWS (Feb. 20, 2019), https://www.apnews.com/ddfa055f09e842bdbbbd38c2fba74a1a. This proposition comes after a history of Maryland's distaste for familial DNA searching: Maryland is one of only two jurisdictions in the country that bans familial searching in government databases, and the only state to ban searches for blood relatives. *See id.*

99 *See id.*

100 *See id.*

101 *See* Murphy, *supra* note 80.

a genetic profile without a warrant violates the Constitution."[102] In that case, which is unique in that the crime had only been committed three years prior to the use of the commercial DNA database in the defendant's arrest and prosecution, the defendant argued that he did not knowingly expose his DNA profile to the public by submitting it to a commercial DNA database.[103] Because the government did not obtain a warrant, he argued, this was an unreasonable search under the Fourth Amendment—comparable to searching the contents of a cellphone, which the Supreme Court has ruled is an unreasonable search that requires a warrant.[104] However, the judge denied this motion, and the defendant pled guilty in October of 2019.[105]

The Supreme Court most recently addressed Fourth Amendment rights in *Carpenter v. United States*, in which the Court held that individuals have a reasonable expectation of privacy in data recovered from cellphone towers that shows their movements.[106] *Carpenter* was the latest in a long line of Supreme Court decisions struggling with technology and its implications for constitutional rights.[107] The Court's consideration of *Carpenter* sparked speculation as to whether it might soon take a case regarding law enforcement access to commercial DNA databases.[108] However, with the narrow ruling in *Carpenter*, it is unclear what the Court might decide.

The question here is whether genealogy companies are constitutionally permitted to share this information with law enforcement

---

102 Rachel Weiner, *Alexandria Rape Suspect Challenging DNA search Used to Crack Case*, WASHINGTON POST (June 10), https://www.washingtonpost.com/local/public-safety/alexandria-rape-suspect-challenging-dna-search-used-to-crack-case/2019/06/10/24bd0e34-87a5-11e9-a870-b9c411dc4312_story.html?utm_term=.a80ac9b4d330.

103 *See id.*

104 *See id.*

105 *Bjerke Convicted of Rape and Firearms Offenses*, City of Alexandria (Oct. 18, 2019), https://www.alexandriava.gov/commattorney/info/default.aspx?id=111830.

106 Carpenter v. United States, 138 S.Ct. 2206, 2217 (2018).

107 *See e.g.*, Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that when the Government uses a device that is not in public use to explore the details of the home that would have been unobservable without physical intrusion, the surveillance is a "search" and presumptively unreasonable without a warrant); Riley v. California, 573 U.S. 373, 386 (2014) (holding that officers must generally secure a warrant before conducting a search of data on cell phones); United States v. Jones, 565 U.S. 400, 404 (2012) (holding that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a "search").

108 *See* Ford, *supra* note 25.

without running afoul of the customer's Fourth Amendment rights. The answer to that question lies in the "third-party doctrine" of the Fourth Amendment.[109]

II. FOURTH AMENDMENT PROTECTIONS

The Fourth Amendment of the United States Constitution provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[110] This protection has been scrutinized and clarified ever since its inclusion in the Constitution, and the Supreme Court has provided guidance on what constitutes a search or seizure in the first place under the Fourth Amendment.

One of the most important clarifications was provided by the Court in *Katz v. United States*.[111] In *Katz*, the Court first articulated what it means to have a "reasonable expectation of privacy," and how that expectation dictates what constitutes an unreasonable search under the Fourth Amendment.[112] Over time, the Court has confirmed that a reasonable expectation of privacy is both subjective and objective, meaning that the person seeking privacy must actually expect privacy *and* that expectation must be reasonable to society.[113] Thus, if a warrantless government search

109 *See infra* Analysis Section 1.

110 U.S. Const. amend. IV.

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

112 *See id.* at 351-52. In this case, the Court abandoned the old understanding of what the Fourth Amendment protected (the trespass doctrine, which only protects tangible items) and restructured its understanding to include intangible privacy interests. The Court essentially moved the focus of the protections from a person's things to people themselves. However, in doing so, the Court simultaneously narrowed the protection of anything that *wasn't* within the privacy expectations of the person, i.e. anything that the person knowingly exposes to the public or another person. *See* RICHARD M. THOMPSON II, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 6 (2014).

113 *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Of course, whether an expectation is reasonable according to society is subject to a number of factors, including the importance of the needs of law enforcement in conducting the search. The Supreme Court balances an individual's right to be free from unreasonable searches and seizures against the needs of law enforcement—the more important those needs, the more reasonable the search. *See* e.g. Maryland v. Buie, 494 U.S. 325, 334 (1990) (holding that a warrant is not required to perform a protective sweep of rooms adjoining the place of arrest in a home where there are

contravenes a person's actual expectation of privacy, and that expectation is reasonable according to society, that warrantless search would be unreasonable under the Fourth Amendment.[114] Because of the Fourth Amendment's "fruit of the poisonous tree" concept, if evidence is obtained through an unconstitutional search it is excluded altogether at trial.[115]

However, this protection against warrantless, unreasonable searches has been subject to many exceptions and conditions over time. One of these exceptions is the "third-party doctrine."[116] The third-party doctrine declares that a person who voluntarily gives information to a third party has *no* reasonable expectation of privacy in that information because he assumes the risk of disclosure to other parties.[117] Thus, if a person shares information with a company or third party, that person should no longer reasonably expect that the information is private, and the police no longer need a warrant to obtain it.[118] The Fourth Amendment only prohibits *unreasonable* searches—a warrantless search of property that someone has given away is not unreasonable.[119]

Further, the third-party doctrine exception extends even to information that is "revealed on the assumption that it will be used only for a limited purpose."[120] This extension was justified by the Court because it is the original who takes a risk in revealing his information to a third party and thus he cannot expect the information will not be given to the government, or any other party, for additional purposes.[121]

"articulable facts which, taken together with the rational inferences from those facts, would warrant a reasonably prudent officer in believing that the area to be swept harbors an individual posing a danger to those on the arrest scene.").

114 *See Katz,* 389 U.S. at 361 (Harlan, J., concurring).

115 *See* Weeks v. United States, 232 U.S. 383, 398 (1914) (holding that the use of letters obtained by an unconstitutional search at trial was a "prejudicial error"); *see also* Mapp v. Ohio, 367 U.S. 643, 655 (1961) (holding that all evidence obtained by searches and seizures in violation of the Constitution is inadmissible in a state court).

116 *See* THOMPSON II, *supra* note 111.

117 *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

118 *See id.*; *see also* United States v. Miller, 425 U.S. 435, 443 (1976).

119 *See Smith*, 442 U.S. at 743-44.

120 *Miller*, 425 U.S. at 443.

121 *See id.* In *Miller*, law enforcement requested access to the defendant's bank records and other financial information without obtaining a warrant to gain evidence of his alleged crime. The Court reasoned that because the defendant had voluntarily given his information to the bank, the bank was free to disseminate it to the government if it wished. *Id.*

Recently, however, the Court has been narrowing the third-party exception as technology has become more prevalent in peoples' lives and private information becomes more difficult to keep to one's self.[122] For example, in *Carpenter*, the Court held that cell-site records,[123] because of the "nature of the particular documents sought," were protected by Fourth Amendment rights and did not fall within the third-party doctrine, even though they were technically given to the phone company, which was a third party.[124] The court dictated three main reasons for this decision. While the first reason was more specifically related to location information, the second two reasons analyzed the type of information sought and whether the third-party doctrine applied.

First, the Court explained that it is already well-established that individuals have a reasonable expectation of privacy in their physical movements, which applied to the information the cell-site location provided.[125] The Court explained that the amount of information a phone carries documenting the user's presence at every moment of every day is a new-age privacy concern that is protected by the Fourth Amendment under clear precedent.[126]

Next, the Court considered the amount of "identifying information" in the property searched in order to determine whether there is a legitimate expectation of privacy in the property.[127] The Court found that the vast amount of identifying information in cell-site location tracking was too intrusive to be considered standard, business-related information—that is, the type of information normally excepted by the third-party doctrine.[128] The Court explained that if information as detailed as one's location at every second of every day was included within the scope of the third-

122 *See* Carpenter v. United States, 138 S.Ct. 2206, 2214 (2018) ("As technology has enhanced the government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (Quoting *Kyllo v. United States*, 533 U.S. 27, 34 (2001))).

123 Cell-site records are the records a phone company keeps about a person's location according to his cell phone. *See id*. at 2225.

124 *Id*. at 2219.

125 *Id*. at 2217.

126 *Id*. ("As with GPS information, the timestamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations.").

127 *Id*. at 2219 (citing *Smith*, 442 U.S. at 742; *Riley*, 134 S.Ct. at 2493).

128 *See id.*; *see also Miller*, 425 U.S. at 442.

party doctrine, the doctrine would lose its original justification.[129] After all, the doctrine was meant to be an exception for the government to gain access to documents that record a singular act or set of acts conducted with or through the third party—not an unlimited backdoor into the most intimate parts of one's day-to-day activities and everyday actions.[130]

Finally, the Court considered the voluntariness of the exposure to the third party by the owner.[131] The Court, in the past, has explained that it would be unreasonable to freely give one's information away to third parties but still expect that information to remain private and within the scope of the *owner's* intended audience.[132] But in *Carpenter*, the Court recognized that "[c]ell phone location information is not truly 'shared' as one normally understands the term" for the purposes of the third-party doctrine, and thus does not fall neatly into the original justification for the exception.[133] Here, the Court drew an important distinction between information affirmatively disseminated to the third party and information that is taken from the person by the third party, albeit consensually, but only collaterally with the original purpose of the contract.[134] In other words, the Court differentiated between information actively given and information passively given without any specific action from the person. The root of the "voluntariness of exposure" justification hinges on the fact that the owner assumed the risk of disseminating his information to the third party.[135]

A cellphone automatically logs the location of the user without any affirmative action by him, seriously diminishing his part in sharing the information and, therefore, making it less likely that he assumed any risk.[136] The Court ruled that because cell phone companies collect location information collaterally and are not affirmatively given that information, "in no meaningful sense does the user voluntarily 'assume the risk' of turning over a

129 *See Carpenter*, 138 S.Ct. at 2221-22.
130 *See id.* at 2219, 2223.
131 *See id.* at 2220.
132 *See Miller*, 425 U.S. at 443.
133 *Carpenter*, 138 S. Ct. at 2220.
134 *See id.*
135 *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).
136 *See Carpenter*, 138 S. Ct. at 2220 ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.").

comprehensive dossier of his physical movements."[137] Further, the Court explained that having a phone in this day in age is integral in a person's life.[138] Thus, it would be unfair and unreasonable to expect a person to forego having a cell phone just to opt-out of sharing his location with the government at all times.

Notwithstanding its decision in *Carpenter*, the Supreme Court has consistently and historically held that the third-party doctrine exception applies to information that the person assumes or is told will not be given to the government or *another* third party.[139] The assumption of risk is still present when someone gives his information away, no matter how comfortable he is in the third party's trustworthiness.[140] The Court has explained that the Fourth Amendment to the United States Constitution "does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[141]

Lastly, the Supreme Court noted that its decision in *Carpenter* is a narrow one and does not disturb the decisions in *Smith v. Maryland*[142] or *United States v. Miller*,[143] the Court's two most important decisions regarding the third-party doctrine; the *Carpenter* decision solely applies to real-time cell-site location information.[144] Thus, the third-party doctrine precedent before this case remains theoretically untouched. Regardless, some constitutional law commentators believe the Court is hinting at narrowing the third-party doctrine as technology continues to advance.[145]

137 *Id.* (quoting *Smith*, 442 U.S. at 745).
138 *See id.*
139 *See* United States v. Miller, 425 U.S. 435, 443 (1976).
140 *See id.*
141 *Id.*
142 *See Carpenter*, 138 S. Ct. at 2220.
143 *Id.*
144 *See* Carpenter v. United States, 138 S.Ct. 2206, 2220 (2018). Instead of altering the third-party doctrine analysis laid out by the Supreme Court through precedent, the Court explained that this type of information (cell-site location information) simply falls *outside* the exception. However, because it is the first of its kind in terms of new technology, it is unclear what other types of new technology would fall outside the exception and what types would still fall within. *See id.*
145 *See* Ford, *supra* note 25; Jake Laperruque, *The Carpenter Decision: A Step Forward for Privacy Rights but Major Problems Remain*, POGO (June 28, 2018),

III. LAW ENFORCEMENT USE OF COMMERCIAL DATABASES IS CONSTITUTIONAL

Law enforcement access to commercial DNA databases, albeit limited to investigations of violent or sexual assault crimes, should be held constitutional under the third-party doctrine of the Fourth Amendment because the small expectation of privacy left in information derived from samples of DNA voluntarily given to a third party is outweighed by law enforcement's great need to effect investigations into these types of crimes. In the balance between privacy rights and public safety, the expectation of privacy in information disseminated to a third party is too low, if it exists at all, in comparison to the government's interest in solving the alarming number of unsolved violent crimes.

A. Expectations of Privacy of Both the Customer and the Target are Low or Nonexistent.

In general, there are two parties who may be affected by law enforcement's use of commercial DNA databases: the eventual target of the search—the suspect—and the person who submitted the DNA to the database—the genealogy customer. As explained above, in familial searches, those parties are not always the same person. Of course, there are times when the suspect in a case will have submitted his own DNA to a commercial DNA database, and a search of the database reveals that his DNA matches the law enforcement-submitted sample, producing an exact suspect match. This scenario makes the target of the DNA search and the genealogy customer, or the owner of the sample, the same person—thus the target and genealogy customer necessarily possess the same rights. However, when the target and the genealogy

https://www.pogo.org/analysis/2018/06/carpenter-decision-huge-step-forward-for-privacy-rights-but-major-problems-remain. ("This will have major ramifications not just for other Fourth Amendment cases involving smartphones, but also involving a host of other technologies. From now on, the standard of "voluntarily" giving up data is not whether it was technically possible to instead live in a hut off the grid, but rather whether such data stems from a necessary action to participate in modern society."). *See* Michael Bahar, et. al., *Third Party-Crashing? The Fate of the Third-Party Doctrine*, LAWFARE (Oct. 19, 2017), https://www.lawfareblog.com/third-party-party-crashing-fate-third-party-doctrine.

customer are separate people, they possess separate rights. Part III(A)(i) will address the genealogy customer's Fourth Amendment rights—whether or not he is also the target. Part III(A)(ii) will address the target's Fourth Amendment rights when he is *not* also the customer.

i. Expectation of the Genealogy Customer

There is very little (if any) expectation of privacy in property disseminated to a third party.[146] In the context of governmental searches of commercial DNA databases, the government would not violate the customer's Fourth Amendment rights by using this method of searching because it falls within the third-party doctrine exception. Before *Carpenter*, there was no question as to whether the law would allow for a commercial DNA database to disseminate volunteered information about its customers because the customers had given such information to the third-party commercial database company.[147] But even though *Carpenter* narrows that exception, information derived from DNA samples given to third party companies still falls well within the third-party doctrine exception because this type of evidence is distinguishable from the evidence in *Carpenter*.

As discussed in the previous section, *Carpenter* created a more updated analysis that incorporated technology into a historically non-technological exception to the warrant requirement. One of the points of analysis—sharing of location information—is irrelevant to this discussion.[148] Thus, the analysis here is focused on the

146 *See Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 743-44; *Carpenter*, 138 S.Ct. at 2216.

147 *See Miller*, 425 U.S. at 443; *Smith* 442 U.S. at 742-43.

148 The first prong of the analysis in *Carpenter*—the fact that the information involved the subject's location—is irrelevant to this analysis because here, DNA information does not necessarily involve an individual's location. While a DNA sample in a specific place may provide circumstantial evidence that a person was present there at some point, DNA does *not* provide information as to a person's whereabouts at a specific time. Location information privacy has been thoroughly litigated and has clear precedent, which is why the Court ruled partially on those grounds—separate from its third-party doctrine analysis. The Court has already held that an individual's GPS location is private and that a warrant is needed for the government to obtain a digitally-created map of a person's whereabouts. *See* United States v. Jones, 565 U.S. 400, 404 (2012). Thus, because DNA information does not give the government access to a person's continual whereabouts, that part of the analysis does not apply here.

remaining two points: the pervasiveness of the identifying information involved in the search and the voluntariness of the exposure of the subject of the search.

First, while one's DNA can certainly be used to identify a person through investigatory means, DNA is *not* considered "identifying information" under United States law because it does not actually identify someone without additional samples, as opposed to evidence such as medical records.[149] Thus, it is a different type of identifying information than the location information in *Carpenter*, which fell outside the third-party doctrine exception. The information at issue in *Carpenter*, if given to the government, would alone have provided law enforcement with an unlimited amount of information that revealed where the defendant had been at any point of any day.[150] Without needing any additional information, law enforcement would acquire an unreasonable amount of intrusive information in their investigation of the defendant.

Contrarily, access to information derived from DNA samples is much more similar to the snapshot-like information[151] obtained in *Smith v. Maryland*, where the Supreme Court decided the third-party doctrine applied: a piece of data about a single point in time instead of a live stream of continuous identifying information.[152] In fact, a DNA sample can be more adequately compared to a fingerprint than to a live stream of someone's location.[153] Instead of gaining access to real-time surveillance of the target of the search, law enforcement is accessing a "fingerprint" of sorts, identifying a certain person that can be linked to another "fingerprint" of the

149 Chelsea Whyte, *Family-Tree Forensics*, NEW SCIENTIST (August 11, 2018), https://web-a-ebscohost-com.jerome.stjohns.edu/ehost/delivery?…2540sdc-v-sessmgr01%26bdata%3dJnNpdGU9ZWhvc3QtbGl2ZQ%253d%253d ("Despite uniquely identifying you, DNA records are considered in US law to be de-identified information that can be given to police without a court order.").

150 *See Carpenter*, 138 S.Ct. at 2220 ("[T]his case is not about 'using a phone' or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years.").

151 In *Smith*, law enforcement gained warrantless access to the list of phone numbers dialed by the defendant. The Court argued that because this information was not as intrusive as listening in on a conversation or recording what was being said and was instead simply a record of who he had called, the third-party doctrine applied. *Smith*, 442 U.S. at 743-44.

152 *See id*. at 743 ("Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed.").

153 *See* National Institute of Justice, *Using DNA to Solve Cold Cases,* U.S. DEPARTMENT OF JUSTICE (Jul. 2002), https://www.ncjrs.gov/pdffiles1/nij/194197.pdf.

same person if another were to be acquired. These "fingerprints" are *not* as intrusive as cell-site location information because they do not give law enforcement access to one's whereabouts at all times; they merely tell law enforcement that the owner of the "fingerprint" may have been present at a particular crime scene at some point. Of course, DNA profiles are unique to each individual, but they are not maps of a person's life; they are simply coded name tags that do not contain any identifying information on their own.

Next, the DNA samples in commercial DNA databases were unquestionably given affirmatively and voluntarily. Not only do people send in their DNA samples to the companies, but they pay the company to specifically analyze their DNA samples to report back identifying information about the customers.[154] In *Carpenter*, the Court ruled that it would be unreasonable to include location information in the third-party doctrine because people are not affirmatively sending in their location when they buy a cell phone; it is just something that is recorded when one owns a phone.[155] This is completely distinguishable from the act of sending a company one's DNA sample. The affirmative action—in fact, the *only* action—one takes in contracting with commercial DNA databases is the voluntary dissemination of one's DNA and the information attached to it. Instead of being a collateral part of the transaction, giving the company one's DNA is the entirety of the transaction.

Further, sending DNA to a company for genealogical purposes is certainly not a "pervasive and insistent"[156] part of daily life as the Court meant it in *Carpenter*. Taking this action is nowhere near as integral in someone's life as owning a cell phone. It would be much more reasonable to simply forego paying for a genealogy service if one did not want a third party to have information derived from his DNA than it would be to expect someone to forego owning a cell phone for the same reason. Therefore, DNA samples in commercial databases are voluntarily and affirmatively shared for the purposes of the third-party doctrine.

154 *See* 23andMe *supra* note 44; AncestryDNA FAQ *supra* note 44.

155 *See Carpenter*, 138 S.Ct. at 2220 ("[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. . . . Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.").

156 *Id.* (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

Finally, the fact that the information is given to these companies for the limited purpose of analyzing the DNA and conducting a familial search does *not* preclude the information from falling within the third-party doctrine.[157] As the Court in *Miller* explained, someone's belief and trust that the information he gave away will only be used for the purpose for which he gave it away is a risk he takes to his own detriment.[158] This, it follows, would still be the case even if companies claimed to prohibit law enforcement from submitting the DNA sample of a suspected criminal from a crime scene.[159] Once a company decides to disseminate the information it was given, it would be theoretically free to do so.[160] Thus, the fact that customers did not give samples of their DNA with the expectation that they would be searched by law enforcement is not a reason to preclude law enforcement from gaining access.

157 *See Miller*, 425 U.S. at 443.

158 *See id*.

159 Some companies include in their policies a promise to not disseminate information to law enforcement, or a concession that in certain circumstances, they will. *See, e.g.*, 23andMe, *Privacy Highlights*, https://www.23andme.com/about/privacy/ (last updated Oct. 30, 2020) ("We will not provide information to law enforcement or regulatory authorities unless required by law to comply with a valid court order, subpoena, or search warrant . . . ."). While this theoretically does not alter whether or not they may "change their minds" and do so within the scope of the Fourth Amendment third-party doctrine, it may affect the Court's decision as to whether or not someone's expectation of privacy in the information was legitimate and reasonable. For example, a person who only submitted his DNA sample to a company that promised not to cooperate with law enforcement may have a better argument as to his legitimate expectation of privacy than someone who disseminated his information to a company that did not specify whether it would or a company that specified that it would.

160 *See Miller*, 425 U.S. at 443. It is worth noting that for those commercial DNA databases that promise not to comply with law enforcement in their policy statements, other laws outside the scope of this note may determine whether or not that company is free to refuse compliance. The third-party doctrine of the Fourth Amendment is only applicable when determining whether or not a company *may* cooperate with law enforcement to begin with. Procedures that involve non-cooperation of the companies are outside the scope of this note.

ii. Expectation of the Target

There is no expectation of privacy in someone else's property.[161] Thus, when the target of a familial search is identified using someone else's DNA profile—namely, a relative's—the target cannot assert that he had an expectation of privacy in that relative's DNA. According to the Supreme Court, "Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted."[162] The Court made clear in *Alderman v. United States* that one's rights must have been personally violated in order to claim a Fourth Amendment violation and assert the exclusion of evidence; it is not enough for the person to have simply been negatively affected by the introduction of damaging evidence.[163] The Court has also stated that "[i]n order to qualify as a 'person aggrieved by an unlawful search and seizure,' one must have been a victim of a search . . . as distinguished from one who claims prejudice only through the use of evidence gathered as a consequence of a search or seizure directed at someone else."[164]

For example, if someone's house is unconstitutionally searched by the government, that person can claim a violation of his constitutional rights.[165] However, if evidence is found during that unconstitutional search that incriminates someone else—like if someone who does not live in the house hides drugs in the homeowner's drawer—the incriminated person cannot claim that his Fourth Amendment rights were violated.[166] The government did not search *his* property and therefore his rights were not threatened.[167]

When law enforcement uses familial searching to find family

161 *See* Rakas v. Illinios, 439 U.S. 128, 133-34 (1978).

162 *Id.* (quoting Alderman v. United States, 394 U.S. 165, 174 (1969)).

163 *Alderman*, 394 U.S. at 171 (holding that the exclusionary rule did not apply to the petitioner in the case of an illegal wiretapping because he was not the subject of the search).

164 Jones v. United States, 362 U.S. 257, 261 (1960), *overruled by* United States v. Salvucci, 448 U.S. 83 (1980).

165 *See Alderman*, 394 U.S. at 173.

166 *See Salvucci*, 448 U.S. at 85.

167 *See Alderman*, 394 U.S. at 174. Further, the homeowner could not suppress the evidence being used against the incriminated person; even though the homeowner's rights were violated, the only person who can suppress unconstitutionally obtained evidence is the person being criminally charged using evidence that was unconstitutionally obtained *against him*. *See id.* Thus, the suppression of this kind of evidence has to be entirely through the violation of the suppressor's rights.

members of a forensic profile left at the scene of a crime, they are conducting a search of the genealogy customers' DNA, not the suspect himself. Therefore, if familial searching is used to target a suspect and a match in the DNA of the suspect's family is obtained through that search, the target cannot assert a violation of his rights—that right is reserved for the genealogy customer who was searched.[168] Thus, in the "Golden State Killer" case,[169] the defendant would not be able to assert that his rights were violated by the search that resulted in a familial match to his relative's DNA. Moreover, even if the court found that the search of his relative's DNA was unconstitutional as to the relative, that conclusion would be irrelevant to the prosecution of Joseph DeAngelo.[170] However, as discussed, that search would be constitutional regardless.

B. *Public Safety Needs are High*

Even if the Court did find that there is a small but legitimate expectation of privacy in the DNA samples customers give to commercial DNA databases, that expectation would be outweighed by the public safety needs that could be solved through law enforcement's access to these databases. The Supreme Court has repeatedly held that the legitimate needs of public safety are consistently weighed as a factor against the privacy rights in search issues when determining whether a search was reasonable under the Fourth Amendment.[171] The more important the governmental interest, the more likely the Court is to find that the search was reasonable under the circumstances.[172] In fact, the Court has stated

168 *See Salvucci*, 448 U.S. at 85.

169 Ford, *supra* note 25.

170 *See Salvucci*, 448 U.S. at 85.

171 *See e.g.* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 633 (1989) (holding that regulations on toxicology testing of railroad employees covered by the Hours of Service Act did not violate the Fourth Amendment because government interests outweighed the employee's diminished expectation of privacy).

172 *See* Maryland v. Buie, 494 U.S. 325, 331 (1990) (citations omitted) ("It goes without saying that the Fourth Amendment only bars unreasonable searches and seizures. Our cases show that in determining reasonableness, we have balanced the intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.").

that "the permissibility of a particular practice 'is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'"[173]

The government's interest in solving violent crimes using DNA evidence from databases is legitimate, and the use of those databases would greatly promote the government's interest in public safety. First, DNA evidence is unquestionably helpful in investigations of violent crimes.[174] In fact, a study researching the use of forensic evidence in investigations found that when an investigation used scientific evidence, clearance rates[175] were *three times greater* than in cases where scientific evidence was not used.[176] In particular, the Supreme Court has articulated great deference to law enforcement in cases specifically related to the collection of DNA for crime-solving purposes.[177] In fact, the Court has made it clear that "[i]n some circumstances, such as '[w]hen faced with special law enforcement needs, diminished expectations of privacy, minimal intrusions, or the like, the Court has found that certain . . . circumstances may render a warrantless search or seizure reasonable.'"[178]

Law enforcement's access to commercial DNA databases would astronomically benefit law enforcement in solving crimes by giving them access to millions of more profiles to which they could compare a forensic "John Doe" profile left at the scene of a crime. AncestryDNA and 23andMe alone could provide millions of more profiles for comparison.[179] Access to this amount of profiles would be an incalculable benefit to law enforcement's ability to solve cold

173 *Skinner*, 489 U.S. at 619 (quoting Delaware v. Prouse, 440 U.S. 648, 654 (1979)).

174 *See Using DNA to Solve Crimes*, U.S. DEP'T JUST. ARCHIVES, https://www.justice.gov/archives/ag/advancing-justice-through-dna-technology-using-dna-solve-crimes (last updated Mar. 7, 2017) ("When used to its full potential, DNA evidence will help solve and may even prevent some of the Nation's most serious violent crimes."). *See* Morgan & Kena, *supra* note 1 (explaining how violent crimes include sexual assault).

175 A crime is "cleared," generally, when a suspect is arrested for or charged with a reported crime. FED. BUREAU INVESTIGATIONS: UNIFORM CRIME REPORTING, *supra* note 6.

176 Joseph Peterson, et al., *The Role and Impact of Forensic Evidence in the Criminal Justice Process*, U.S. DEP'T JUST. (Sept. 2010), at 1, https://www.ncjrs.gov/pdffiles1/nij/grants/231977.pdf.

177 *See* Maryland v. King, 569 U.S. 435, 461, 465–66 (2013) (holding that the collection of DNA of arrestees charged with serious crimes for crime-solving purposes without a warrant was constitutional under the Fourth Amendment).

178 *Id*. at 447 (quoting Illinois v. McArthur, 531 U.S. 326, 330 (2001)).

179 Levenson, *supra* note 8.

cases for which they have acquired a DNA sample but do not have a match, just like the Golden State Killer case. In just the first year after the detectives in the Golden State Killer case shared the details of their breakthrough, there have been at least three breakthroughs in cold cases using the same familial searching method via commercial DNA databases.[180]

Beyond solving crimes, law enforcement's access to these profiles could actually help *prevent* violent crime. According to a 2012 study, "larger DNA databases reduce crime rates, especially in categories where forensic evidence is likely to be collected at the scene—e.g., murder, rape, assault, and vehicle theft."[181] In the study, the researchers measured the probability of conviction of re-offenders whose DNA profiles had been collected and added to the governmental DNA database and of those whose DNA had not yet been collected.[182] The study found that those offenders whose DNA profiles were already in the database were significantly more likely to be convicted of the crime—i.e., more likely to be caught, which is shown to be a more effective deterrent than a longer sentence.[183]

The study further found that in areas where DNA was collected by the government under additional circumstances—like if that particular state collected DNA for more types of crimes—the crime rates were significantly reduced when this change was implemented. The study estimated that if a database is expanded by twelve percent, that expansion would result in a 3.2% decrease in murders, a 6.6% decrease in rapes, and a 2.9% decrease in aggravated assaults.[184] Most importantly, the study found that "in the United States, DNA profiling makes violent offenders seventeen percent less likely to re-offend."[185] This, in turn, would theoretically have had a deterrent effect on a criminal like the Golden State Killer. The study suggested that increasing the likelihood of

180 *Id.*

181 Jennifer L. Doleac, *The Effects of DNA Databases on Crime*, at 1 (American Economic Association Working Paper, 2012), https://siepr.stanford.edu/sites/default/files/publications/Doleac_DNADatabases_0_5.pdf.

182 *Id.* at 13.

183 *Id.* at 2, 16 ("The probability of reoffending and being convicted for any offense is 3.7 percentage points (23.4%) higher for those with a profile in the DNA database than those without.").

184 *Id.* at 22.

185 Doleac, *supra* note 24.

getting caught significantly deters offenders from re-offending altogether.[186]

Law enforcement's access to commercial DNA databases would create the same deterrent effect as a larger database would for the same reasons. The study makes clear that as long as offenders are affected by the idea of going to prison, "increasing the probability of conviction might be a more cost-effective crime prevention strategy than increasing sentences."[187] As shown in Erlich's study, access to commercial DNA databases would give law enforcement a substantially higher chance of finding a match for the crime scene sample, since more than half of the people in the study were linked in the commercial databases.[188]

It follows, of course, that identifying perpetrators more often could not only create a deterrent effect among repeat offenders but could incapacitate more would-be repeat offenders before they ever had the chance to re-offend. If the Golden State Killer had been caught and incapacitated sooner, he would not have had the chance to commit as many horrible crimes as he did, deterred or not. Thus, not only could law enforcement's access to commercial DNA databases help solve violent crimes—it could prevent the crimes from happening altogether.

C. Privacy Advocates' Arguments are Misguided

Of course, there are proponents of individuals' privacy rights who argue this method of searching is an invasion of privacy and should be prohibited by the Fourth Amendment, despite the high benefit to law enforcement. These individuals argue that this exception to the warrant requirement is too broad, and police should be required to obtain a warrant if they want to gain access to the database in order to conduct a search for a match.[189] However,

186 Doleac, *supra* note 181, at 25.

187 *Id.* at 7.

188 Erlich, *supra* note 88.

189 *See* Ronald Bailey, *What the Golden State Killer Case's Use of DNA Means for Your Personal Privacy*, THE ORANGE COUNTY REGISTER (May 24, 2018, 11:50 AM), https://www.ocregister.com/2018/05/24/what-the-golden-state-killer-cases-use-of-dna-means-for-your-personal-privacy; *see also* Cara, *supra* note 86 ("In an ideal world, law enforcement agencies could also still access these services, but only obtaining after explicit permission, such as through a warrant.").

their warrant proposal fails to account for the fact that it would be *impossible* to obtain a warrant to search for a DNA sample from "John Doe," the suspected killer or rapist, or his relative for comparison because the police do not yet know the identity of the person for whom they are searching.[190]

When police use exact suspect or familial searches, they do so precisely because they need to find a name attached to this particular DNA sample *in order to obtain a warrant* for that person's DNA. Obtaining a warrant is impossible before these searches are conducted. Commercial DNA databases have solely been used by law enforcement as an investigative tool in the process of finding a perpetrator—*not* used for obtaining actual DNA from the company.[191] Thus, to make an arrest, the police would still have to go through regular police procedure in obtaining the actual suspect's DNA—all the commercial DNA database gives law enforcement is a closer idea of where to look.

This reality about the investigative process is also the reason why the argument is irrelevant that commercial DNA database information is too unreliable to be legal proof. Law enforcement does not use the information gained from the databases as legal proof. Law enforcement uses these databases to point them in the right direction in order to *obtain* legal proof—just like every other investigative technique. Thus, it does not matter how "unreliable" privacy advocates claim these services to be—if it points to a dead-end, then law enforcement needn't look any further. For example, in the Golden State Killer case, after law enforcement narrowed its pool of suspects down to relatives of the DNA match, they conducted their investigation just as they always would have—and they still had to collect Joseph DeAngelo's DNA sample through a traditional method.[192] The DNA match was simply used to narrow down suspects during the investigation procedure.

Moreover, this argument suggests that if obtaining a warrant is impossible, the next most reasonable requirement would be to force every genealogy customer to obtain the consent of all of his family members who his DNA sample could possibly negatively

190 U.S. Const. amend. IV. "[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing* the place to be searched, and the *persons or things* to be seized." *Id.* (emphasis added).

191 *See* Cara, *supra* note 86.

192 *Id.*

implicate if obtained by law enforcement.[193] But this is nonsensical: people submit their DNA to these companies to *find out* the identities of their relatives in the first place. Forcing people to acquire consent from the very relatives they are seeking to find demonstrates a failure to understand the DNA industry and the third-party doctrine. The law does not require people to seek out every person who could possibly be affected by every personal decision they make; in fact, this is the very reason the third-party doctrine exception exists to begin with.[194]

CONCLUSION

> Fifty-one rapes and twelve murders . . . . It is time for all victims to grieve and take measure one last time. To bring closure to the anguish that we've all suffered for the last 40-some-odd years. It is time for the victims to begin to heal. So long overdue . . . . To the entire reservoir of victims out there: my sadness is with you. For the fifty-one ladies who were brutally raped . . . sleep better tonight . . . he's in jail, and he's history.[195]

These are the words of Bruce Harrington, the brother of one of the people murdered by Joseph DeAngelo. Since his brother's death, Harrington has been an active voice in the push for legislation allowing law enforcement to use DNA evidence more efficiently and effectively to aid their investigations.[196]

---

193 Whyte, *supra* note 149 ("But genetic information is so widely spread that it would be impossible to coordinate consent from everyone who shares your DNA.").

194 *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 582 (2009). The third-party doctrine is meant to eliminate the never-ending chain of varying expectations of privacy based on who has had ownership of a particular item over the course of time. The doctrine is meant to simplify the process by which the expectation of privacy as to a certain thing is evaluated—not make it more complicated.

195 Sacramento County District Attorney's Office, *East Area Rapist Press Conference 2018 04 25*, YOUTUBE (April 25, 2018), https://www.youtube.com/watch?v=DmmK9LQNkoM.

196 Nicole Chavez, *Arrest of alleged Golden State Killer brings 'wave of relief' to survivors and victims' families*, CNN (Feb. 13, 2019, 3:58 PM), https://www.cnn.com/2018/04/26/us/reaction-golden-state-killer-survivors-

If the police have found a constitutional method that allows them to serve justice to these victims, they should be able to use it. If this technology existed in the 1970s and was used by law enforcement, it is possible the Golden State Killer would not have been able to effect the horrific acts he did. If this method were to be used by law enforcement today, it is very likely that police could stop a violent criminal in his tracks. In fact, the use of these databases could prevent that person from committing crimes in the first place.

The fear of law enforcement gaining too much information is valid—but misplaced here. Violent crime affects millions of people over the course of their lifetime, and if law enforcement can investigate and prevent these crimes more effectively, it should.

Under the United States Constitution, law enforcement should be able to access commercial DNA database information. The Supreme Court has confirmed, time and time again, that information disseminated to a third party is not subject to an expectation of privacy by the original owner. In addition, the benefit to the government's interest in protecting the public is too high to be sacrificed for the small expectation of privacy left in information derived from a disseminated DNA sample. Therefore, law enforcement should continue to use this method of discovering suspects and continue finding justice for those who have been blocked from ever getting it thus far. It is time for the United States justice system to use this resource for the betterment of society and the safety of its citizens—to solve and prevent the most violent of crimes.

victims/index.html.