23, Me, and The Police: The Fourth Amendment Implications of Familial DNA Searching

*Jennie F. O'Hara**

Introduction

On April 24, 2018, a seventy-two-year-old man was escorted out of his Citrus Heights, California home in handcuffs.[1] This man, Joseph DeAngelo—now infamously known as the Golden State Killer—will likely spend what remains of his life in prison, finally paying for the rapes and gruesome murders of dozens of victims throughout the state of California in the 1970s and 80s.[2] DeAngelo's crimes had gone unsolved for over four decades, until savvy police investigators—still invested after all of that time—decided to experiment with a newly conceived investigatory technique: familial DNA searching.[3] Using this method, investigators were able to track down DeAngelo by matching DNA he had discarded at the scene of his crimes with the DNA of his distant relative, uploaded to a genealogy website.[4]

From this anecdotal scenario, it is simple to assume that familial DNA searching by police investigators can yield immeasurable positive outcomes. Although this may be true, it is also easy to imagine the myriad of ways in which law enforcement could weaponize this

* George Mason University Antonin Scalia Law School, J.D. expected, 2020. This Comment is dedicated in memory of Michelle McNamara, whose tireless search for justice was integral in the Golden State Killer's ultimate apprehension.

[1] Juan Carlos Guerrero, *TIMELINE: A Look Back at the Golden State Killer's Crime Spree that Lasted a Decade*, ABC7 (May 23, 2018), https://abc7news.com/timeline-looking-back-at-golden-state-killer-crimes/3391867/.

[2] *See* Michelle McNamara, *In the Footsteps of a Killer*, L.A. Mag. (Feb. 27, 2013), https://www.lamag.com/longform/in-the-footsteps-of-a-killer/.

[3] Laurel Wamsley, *In Hunt for Golden State Killer, Investigators Uploaded His DNA To Genealogy Site*, NPR (Apr. 27, 2018, 7:31 PM), https://www.npr.org/sections/thetwo-way/2018/04/27/606624218/in-hunt-for-golden-state-killer-investigators-uploaded-his-dna-to-genealogy-site.

[4] *Id.*; *see also* Melody Gutierrez, *Golden State Killer Suspect's DNA Taken from Car as he Shopped at Hobby Lobby*, S.F. Chron. (June 2, 2018, 10:51 AM), https://www.sfchronicle.com/crime/article/Golden-State-Killer-suspect-s-DNA-taken-from-12961700.php.

level of intrusion against the privacy rights of American citizens. Under the current Fourth Amendment framework, few safeguards are in place that would effectively protect the privacy rights of individuals who actively participate in public genealogy websites.[5] Furthermore, any existing state regulatory protections are sparse and highly varied.[6] In order for both law enforcement and the general public to benefit from the possibilities and potential advantages of familial DNA searching in criminal investigations, the government must implement uniform regulations.[7]

This Comment will suggest the implementation of federal legislation specifically designed to provide strict standards concerning familial DNA searching in criminal investigations. First, this Comment will discuss background concepts and information pertinent to the current framework of the Fourth Amendment as well as the modern use of DNA evidence generally. Specifically, Part I will discuss in detail the Golden State Killer case and investigation, including the use of familial DNA searching that led to DeAngelo's arrest. Part II will provide a historical overview of the use of DNA analysis in police investigation, including its current utility as an investigative tool. Part III will provide a general overview of Fourth Amendment jurisprudence, defining the scope of the law regarding search and seizure. Part IV will address the business operations of several popular genealogy websites, delving particularly into the privacy and general use disclosures supplied to people who utilize the websites' services. Part IV will also analyze the current landscape of federal regulation with regard to familial DNA testing of genealogy websites. Finally, Part V will conclude the background section by focusing on Colorado's familial DNA searching regulations and policies, as the leading state in terms of this technology.

Next, this Comment will analyze the Fourth Amendment implications surrounding the use of genetic information in the Golden State Killer investigation under the current regulatory scheme. This Comment will then apply the same facts to the Colorado model's framework to determine its effectiveness in real-world scenarios. Finally, this Comment concludes that it is necessary for Congress to enact fur-

---

[5] *See* Michelle Hibbert, *DNA Databanks: Law Enforcement's Greatest Surveillance Tool?*, 34 WAKE FOREST L. REV. 767, 779-81 (1999).

[6] *See id.*

[7] *Id.* at 781-82.

ther legislation to regulate the use of private individual genetic information at the federal level, and specifically suggests federal implementation of the Colorado model.

BACKGROUND

I. THE GOLDEN STATE KILLER

In the early morning hours of June 18, 1976, a twenty-three-year-old woman lay on the floor of her Rancho Cordova, California bedroom with her hands bound behind her back.[8] Despite her bindings, she was able to reach her telephone and call the police, to whom she recounted her horrific ordeal in vivid detail.[9] She stated that she awoke to a man "about five nine, moderately muscular, wearing a navy blue, short-sleeved T-shirt and gray canvas gloves" standing in the doorway of her bedroom, wearing a tight white ski mask to disguise his face.[10] This man went on to rape her before ransacking her home and fleeing the scene.[11] Investigators soon discovered that this man was careful and calculated in the planning and execution of his crimes.[12] They also discovered that he was incredibly cautious not to reveal his identity to his victims.[13]

This man's meticulous nature would prove effective, as this fateful night would go down in infamy as the beginning of his horrifying rampage throughout California over the next decade.[14] What began in 1972 as home invasions quickly turned into rapes, which became violent rapes and tortures, and, eventually, murders.[15] Because of the multi-jurisdictional nature of his crimes throughout California, investigators were initially unaware that they were perpetrated by a single offender.[16] This allowed the offender to commit his crimes undetected

---

[8] MICHELLE MCNAMARA, I'LL BE GONE IN THE DARK: ONE WOMAN'S OBSESSIVE SEARCH FOR THE GOLDEN STATE KILLER 52-53 (Harper Perennial 2019) (2018).

[9] *Id*.

[10] *Id*. at 53.

[11] *Id*.

[12] *Id.* at 54.

[13] *See generally id.*

[14] *See* Guerrero, *supra* note 1.

[15] Emily Shapiro, *Inside the Timeline of Crimes by the 'Golden State Killer'*, ABCNEWS (Apr. 26, 2018, 1:34 PM), https://abcnews.go.com/US/inside-timeline-crimes-golden-state-killer/story?id=54744307.

[16] MCNAMARA, *supra* note 8, at 4.

from 1972 to 1986 before inexplicably vanishing into thin air.[17] The elusive villain stalking California homes received many monikers during that span of time, including—"The Cordova Cat Burglar," "The Visalia Ransacker," "The East Area Rapist," and "The Original Night Stalker."[18] Decades later, after forty-two years, investigators across the state would finally learn that all of these widespread atrocities were the work of a single man: Joseph DeAngelo, the Golden State Killer.[19]

The last known crime attributed to the individual who would become the Golden State Killer occurred in 1986, an era of infantile forensic DNA technology.[20] Although the killer had "left his DNA all over the place"[21] at each crime scene, forensic analysts at the time did not possess the necessary technology to yield any viable leads.[22] It was not until 2011, after years of failed attempts, that police were able to use the DNA left at the crime scenes to create a general profile of the killer.[23] Nevertheless, this profile was not a match with any of the known felons in the Combined DNA Index System (CODIS), the Federal Bureau of Investigation's (FBI) DNA database.[24]

However, many who studied and investigated this case in great detail still believed that pursuing DNA evidence was the best way to "get out of the maze of the Golden State Killer."[25] One such individual was Michelle McNamara, the late author of the novel, *I'll Be Gone in the Dark: One Woman's Obsessive Search for the Golden State Killer*.[26] After McNamara suddenly passed away while writing this novel, her assistants and fellow researchers used compilations of her notes, research, and hard drives to continue her diligent work.[27] In

---

17 *See id*. at 328.

18 Joseph Serna & Benjamin Oreskes, *Why did it Take so Long to Arrest the Golden State Killer Suspect? Interagency Rivalries, Old Technology, Errors and Bad Luck*, L.A. TIMES (May 25, 2018, 4:35 PM), http://www.latimes.com/local/lanow/la-me-ln-golden-state-killer-case-20180525-story.html#.

19 *Id.* The offender has come to be known as "The Golden State Killer," first coined by author Michelle McNamara in a 2013 Los Angeles Magazine article. *See* McNamara, *supra* note 2.

20 Wamsley, *supra* note 3.

21 *Id.*

22 *See id.*

23 MCNAMARA, *supra* note 8, at 144-45; *see also* Wamsley, *supra* note 3.

24 MCNAMARA, *supra* note 8, at 144-45, 302; *see also* Wamsley, *supra* note 3.

25 *See* MCNAMARA, *supra* note 8, at 306.

26 *See generally id.*

27 *Id.* at 283.

those notes, McNamara stated that she believed one potentially fruitful path for DNA analysis was through familial DNA searching.[28] Her notes recognized that although CODIS could not match the crime scene DNA to the Golden State Killer himself, if a member of the perpetrator's family happened to be in the system, police could potentially see a match in trace DNA markers shared by close family members.[29] Even though this line of inquiry rendered no useful results at that initial stage, after just a few more years of dedicated research into the field of DNA technology, this idea would ultimately prove to be the key to solving the case.[30]

On April 24, 2018, just shy of forty-two years after the Golden State Killer's first attack, police in Citrus Heights—a suburb of Sacramento, California—arrested seventy-two-year-old Joseph DeAngelo in his home.[31] Under a familial DNA-driven line of inquiry, California law enforcement had developed a new tactic—familial searching through a "no-frills" site used by amateur genealogists called GEDmatch.com (GEDmatch).[32] Authorities began using GEDmatch, a public genealogical database used to search for relatives and ancestors online, after the traditional route of searching through state and federally run criminal DNA databases did not yield results.[33] According to longtime Contra Costa County District Attorney investigator Paul Holes, after authorities uploaded the Golden State Killer DNA profile to the site, they were able to obtain an extended list detailing the extent to which the DNA uploaded by various individuals on GEDmatch resembled the DNA of the killer—the closer the match in DNA sequences, the more closely related the individuals are.[34] Because GEDmatch users willingly upload their DNA profiles to the site for public use, authorities did not need a court order to access the familial data.[35]

From these results, Chief Deputy District Attorney Steve Grippi stated that police were able to "zero in on DeAngelo" using a DNA

---

28 *See id*. at 286-87, 306.

29 *Id.* at 309.

30 *See* Gutierrez, *supra* note 4.

31 *See* Guerrero, *supra* note 1.

32 *See* Wamsley, *supra* note 3.

33 *Id*.

34 Erik Ortiz, *Golden State Killer Suspect's Capture Sparks DNA Site Privacy Fears*, NBCNEWS (Apr. 27, 2018, 1:49 PM), https://www.nbcnews.com/news/us-news/golden-state-killer-suspect-s-capture-sparks-dna-site-privacy-n869661.

35 *See* Wamsley, *supra* note 3.

profile uploaded by a distant relative.[36] Once authorities had a small pool of possible suspects derived from the public GEDmatch profiles, investigators used the results to explore these family trees and find men who were roughly the right age and height, and were living in California when the crimes occurred.[37] From this point, police were able to hone in on DeAngelo.[38] Specifically, investigators obtained samples of DeAngelo's DNA from his car door handle while he shopped at a local craft store, as well as from a tissue discarded in his trash.[39] Finally, after decades of tireless searching by authorities across the state of California, the Golden State Killer had a name and a face.

When news sources began to report that law enforcement used a public genealogy website to solve a murder investigation, the public's reaction to this revelation was mixed, at best.[40] A large portion of the populace seemed to have been unaware that the information uploaded to databases such as GEDmatch "could later be used to incriminate a relative."[41] As Joel Winston, a New Jersey consumer protection lawyer and former deputy state attorney general, opined, "DNA databases are relatively new, but nobody thinks they'll ever be used in [that] manner."[42] Potential ethical concerns aside, scholars and law enforcement alike have been left to wonder about the legality of using DNA samples from genealogy companies to investigate crimes. State privacy laws may carry some weight, but they are often rebutted because most, if not all, DNA samples supplied to genealogy websites are voluntarily submitted.[43] Because of the inherent infringement these searches have on individual privacy, however, it is imperative to consider the Fourth Amendment implications of this policy.

---

36 *Id.*

37 *Id.*

38 *See* Ortiz, *supra* note 34.

39 *See* Gutierrez, *supra* note 4.

40 *Privacy Concerns After Public Genealogy Database used to ID "Golden State Killer" Suspect*, CBSNEWS (Apr. 27, 2018), https://www.cbsnews.com/news/privacy-concerns-after-public-genealogy-database-used-to-id-golden-state-killer-suspect/.

41 *Id.*

42 Ortiz, *supra* note 34.

43 *Id.*

II. HISTORY OF THE USE OF DNA EVIDENCE IN POLICE INVESTIGATIONS

A. *British Development of the Method*

The use of DNA evidence in its modern form did not arise publicly in the court system until 1986 when Dr. Alec Jeffreys, a geneticist at the University of Leicester, United Kingdom, proposed the radical idea that his recently developed method of genetic testing could be used to apprehend criminals.[44] Jeffreys discovered his method accidentally—the result of a failed attempt at studying the progression of illness through family lineage—when he attached DNA that he had extracted from human cells to photographic film and allowed the film to develop.[45] Each developed film reel bore the image of a unique sequence of bars, which Jeffreys soon realized allowed him to distinguish between the DNA patterns of different individuals with extraordinary precision.[46] Initially, Jeffreys' technique was used as a means to establish the paternity of various children in British immigration disputes.[47] However, police officers soon requested Jeffreys' assistance in identifying the perpetrator behind the rape and murder of two teenage girls in the village of Narborough, Leicestershire, who had managed to evade capture for over two years.[48] After a local teenage boy named Richard Buckland confessed to the crimes, but shortly thereafter recanted, Jeffreys was tasked with comparing the blood and semen the killer left at the crime scenes with a sample of Buckland's DNA.[49] Jeffreys' method led to Buckland's exoneration, as the results confirmed that although the two girls were killed by the same man, that man was not Buckland.[50]

This setback did not hinder police enthusiasm to find the killer, however, and investigators continued pursuing the possibilities Jeffreys' innovative method offered.[51] Police began collecting voluntary

---

44 *See* Ian Cobain, *Killer Breakthrough—the Day DNA Evidence First Nailed a Murderer*, THE GUARDIAN (June 2, 2016, 10:25 AM), https://www.theguardian.com/uk-news/2016/jun/07/killer-dna-evidence-genetic-profiling-criminal-investigation.

45 *Id.*

46 *Id.*

47 *Id.*

48 *Id.*

49 *Id.*

50 *See* Cobain, *supra* note 44.

51 *Id.*

blood samples from men throughout the neighborhood, and eventually amassed a database of over 5,000 samples.[52] However, this too yielded no direct match.[53] It was not until August 1987, over a year since the second victim's body was discovered, that a local man notified police that he had overheard another man in a pub discussing how he had supplied a blood sample on behalf of a workmate named Colin Pitchfork.[54] Police quickly brought Pitchfork in for questioning, and he confessed immediately to the rape and murder of the two young women.[55] For the first time in recorded history, DNA testing had led to the successful conviction of a murderer.[56]

B. *DNA Evidence in the United States*

Dr. Jeffreys' innovative new technique quickly made its way to the United States and began weaving its way into the lexicon of criminal investigative techniques. In 1987, a DNA test was able to confirm that a blood sample extracted from Tommie[57] Lee Andrews perfectly matched traces of semen left at the scene of a rape, leading to America's first DNA-based conviction.[58]

Initially, the admissibility of evidence gained through DNA testing was not frequently disputed in court.[59] However, as prosecutors more widely used the practice as a means to secure convictions, defense attorneys began to question the admissibility of DNA evidence in criminal trials, because they doubted the validity of the techniques used to produce DNA profiles.[60] In 1989, one of the first public challenges against using DNA evidence came before the New York State Supreme Court, Appellate Division, in *People v. Castro*, when the court considered the admissibility of a DNA identification

---

52 *Id.*

53 *Id.*

54 *Id.*

55 *Id.*

56 *See* Cobain, *supra* note 44.

57 Some sources spell Mr. Tommie Lee Andrews' name as "Tommy." *Compare* Andrews v. State, 533 So. 2d 841 (Fla. Dist. Ct. App. 1988) ("Tommie Lee Andrews"), *with* Roger Roy, *DNA Test Gets a Chance in Orange Rape Trial*, THE ORLANDO SENTINEL, Oct. 21, 1987, at A1 ("Tommy Lee Andrews").

58 *See* Karen Cormier at al., *Evolution of DNA Evidence for Crime Solving—A Judicial and Legislative History*, 2 FORENSIC MAG., no. 4 (2005), http://tools.thermofisher.com/content/sfs/brochures/cms_042067.pdf.

59 *Id.*

60 *Id.*

test that would prove that blood found on the defendant's watch belonged to the victim of a murder, tying him directly to the crime.[61] At that time, no appellate court in the state had ruled on the admissibility of DNA evidence in criminal trials, so the court turned to standards for determining the admissibility of new scientific evidence articulated by the U.S. District Court for the District of Columbia in *Frye v. United States* and by the New York Court of Appeals in *People v. Middleton*.[62] The court found that DNA tests satisfied the rule set forth in *Frye*, stating that "the test is not whether a particular procedure is unanimously indorsed [sic] by the scientific community, but whether it is generally acceptable as reliable."[63] In making this determination, the *Castro* court developed a three-prong analysis to aid in its final decision: (1) "Is there a theory, which is generally accepted in the scientific community, which supports the conclusion that DNA forensic testing can produce reliable results?"; (2) "Are there techniques or experiments that currently exist that are capable of producing reliable results in DNA identification and which are generally accepted in the scientific community?"; and (3) "Did the testing laboratory perform the accepted scientific techniques in analyzing the forensic samples in this particular case?"[64] The court was able to discuss the first two prongs with relative ease, concluding first that "[t]here is general scientific acceptance of the theory underlying DNA identification," and second that "DNA forensic identification techniques and experiments are generally accepted in the scientific community and can produce reliable results."[65] Therefore, the court largely decided the case upon consideration of the third prong, holding that "[a] pretrial hearing should be conducted to determine if the testing laboratory substantially performed the scientifically accepted tests and techniques, yielding sufficiently reliable results to be admissible as a question of fact for the jury."[66]

With a clear standard for the admissibility of DNA evidence in court proceedings in place, police and prosecutors were then free to

---

61 People v. Castro, 545 N.Y.S.2d 985 (N.Y. App. Div. 1989).

62 *Id.* at 986 (first citing Frye v. United States, 293 F. 1013 (D.C. Cir. 1923) (discussing the admissibility of blood pressure monitoring to determine honesty during questioning); then citing People v. Middleton, 429 N.E.2d 100 (N.Y. 1981) (discussing the admissibility of bite mark evidence)).

63 *Castro*, 545 N.Y.S.2d at 986-87 (quoting *Middleton*, 429 N.E.2d at 103).

64 *Id.* at 987.

65 *Id*. at 999.

66 *Id.*

develop and utilize the technology within the ever-evolving criminal justice system.[67] In 1989, the Virginia Division of Forensic Sciences became the first state crime laboratory to implement a policy of DNA testing in all of its criminal investigations.[68] The following year, the Virginia General Assembly passed the first state law requiring all individuals with felony convictions to submit DNA samples for inclusion in a state DNA database.[69]

The constitutionality of this state database quickly came into question before the Fourth Circuit in *Jones v. Murray*, one of the earliest cases considering this issue.[70] In *Jones*, the court upheld the constitutionality of Virginia's DNA database system, holding:

> Considering the inmates' questionable claim of privacy to protect their identification and the minimal intrusion resulting from taking a small sample of blood, the Commonwealth's interest in combatting and deterring felony recidivism justifies the involuntary taking of the sample and the creation of the DNA data bank as reasonable in the context of the Fourth Amendment.[71]

Following this favorable decision, each of the other forty-nine states began developing their own DNA database systems—and all fifty states actively maintain their systems through the present day.[72] However, the various state laws creating and regulating the databases are largely inconsistent with one another.[73] For example, four state laws require DNA samples from only those defendants convicted of a felony, while at least eight other states require certain individuals convicted of misdemeanor offenses to also supply DNA samples.[74] Additionally, states inconsistently regulate the procedures through which law enforcement may access the databases.[75] While most states allow for the automatic search of their databases in assistance of criminal

---

67 *See* Hibbert, *supra* note 5, at 774.

68 *Id.*

69 *Id.*

70 Jones v. Murray, 962 F.2d 302, 303 (4th Cir. 1992).

71 *Id.* at 310-11.

72 *See* Hibbert, *supra* note 5, at 775.

73 *Id.* at 779.

74 *Id.* at 776.

75 *See id.* at 779.

investigations, some others are much stricter, allowing police to search the databases only in regard to violent crimes.[76]

In 1990, in an effort to provide a remedy for this inconsistency, the FBI developed CODIS, a streamlined, nationwide database that law enforcement from any state could access.[77] Initially developed as a pilot program implemented in fourteen state and local crime laboratories within the United States, CODIS is now utilized by over ninety crime laboratories across fifty countries.[78] CODIS enables crime laboratories at the federal, state, and local levels to communicate and share information and DNA samples to facilitate effective criminal investigation.[79] In 1994, the DNA Identification Act[80] established the National DNA Index System (NDIS), a national database containing all of the DNA profiles supplied by the federal, state, and local crime laboratories participating in CODIS.[81] Officially implemented in 1998, the NDIS actively participates with all fifty U.S. states, the District of Columbia, and Puerto Rico.[82] The establishment of the NDIS also helped to resolve the inconsistencies resulting from state-by-state laws surrounding access to DNA databases.[83] According to the FBI, "[i]f a state has signed the Memorandum of Understanding . . . to participate in NDIS, that state has agreed to comply with the Federal DNA Identification Act, including the limited access requirements."[84]

---

[76] *Id.*

[77] FED. BUREAU OF INVESTIGATION, *Combined DNA Index System (CODIS)*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis#CODIS-and%20NDIS%20Fact%20Sheet (last visited Oct. 18, 2019) [hereinafter FED. BUREAU OF INVESTIGATION, *CODIS*].

[78] *Id.*

[79] *Id.*

[80] 34 U.S.C. § 12592 (2019).

[81] FED. BUREAU OF INVESTIGATION, *CODIS*, *supra* note 77.

[82] *Id.*

[83] *Id.*

[84] FED. BUREAU OF INVESTIGATION, *Frequently Asked Questions on CODIS and NDIS*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Oct. 18, 2019) [hereinafter FED. BUREAU OF INVESTIGATION, *CODIS and NDIS FAQs*]. The FBI's Memorandum of Understanding is a mandatory agreement for participation in the NDIS, "documenting their agreement to abide by the DNA Identification Act requirements as well as record-keeping and other operational procedures governing the uploading of DNA data, expungements, CODIS users, audits, etc." *Id*.

III. FOURTH AMENDMENT JURISPRUDENCE

A. *Development of Traditional Fourth Amendment Analysis*

The Fourth Amendment to the United States Constitution guarantees:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[85]

Before the Supreme Court's landmark decision in *Katz v. United States* in 1967, courts tended to limit the extension of Fourth Amendment protection to instances in which law enforcement *physically* trespassed on private property to complete a search or seizure, framing the Amendment to focus mainly on property rights.[86] The Supreme Court rejected this viewpoint in *Katz*, holding that the Fourth Amendment "protects people, not places."[87] Specifically, the Court stated, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[88] The Court has upheld that the reasonableness of an expectation of privacy depends on two factors: (1) the individual must have manifested a subjective expectation of privacy in the object of the challenged search; and (2) society must be willing to recognize that expectation of privacy as reasonable.[89] In *Katz*, the Court found that an individual manifests a subjective expectation of privacy in the objects and locations which he seeks to preserve as private.[90] Therefore, if the individual has displayed a reasonable expectation of privacy, the Court will evaluate "whether

---

[85] U.S. CONST. amend. IV.

[86] *See* Katz v. United States, 389 U.S. 347, 352-53 (1967).

[87] *Id*. at 351.

[88] *Id*.

[89] *See* California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing *Katz*, 389 U.S. at 360 (Harlan, J., concurring)).

[90] *See Katz*, 389 U.S. at 351.

the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment."[91]

Because the *Katz* reasonableness standard inherently allows for some case-by-case variation in analysis, the definition of a search or seizure can vary for the purposes of Fourth Amendment protection.[92] However, the Supreme Court has concretely provided that a "search" occurs when an individual manifests a subjective expectation of privacy in something, which society is willing to recognize as reasonable, and that item is observed visually, or by the use of sense-enhancing technology not in general public use.[93] The Court has also stated that a "seizure" occurs "when [an] officer, by means of physical force or show of authority, has in some way restrained the liberty of a citizen."[94] Returning to the significance of the reasonableness consideration, the Court clarified this point to include that "the police can be said to have seized an individual only if, in view of all the circumstances surrounding the incident, a reasonable person would have believed that he was not free to leave."[95]

As previously mentioned, the Fourth Amendment has historically been inextricably linked with property rights.[96] Despite the extension of this point beyond strict property in *Katz*, a trespass analysis is still often invoked in consideration of constitutional protection under the Fourth Amendment. For example, in *United States v. Jones,*[97] the Court ruled in favor of a defendant who had a GPS tracker placed on his vehicle by the government, specifically citing the Fourth Amendment language that notes "[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."[98] The Court reasoned that a person's vehicle is undoubtedly an "effect" as covered under this clause and, therefore, 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."[99] This theory is directly

---

91 *See* Oliver v. United States, 466 U.S. 170, 182-83 (1984).

92 *See Katz*, 389 U.S. at 357.

93 *See* Kyllo v. United States, 533 U.S. 27, 34 (2011).

94 *See* Michigan v. Chesternut, 486 U.S. 567, 573 (1988) (quoting Terry v. Ohio, 392 U.S. 1, 19 n. 16 (1968)).

95 *See id.* (quoting United States v. Mendenhall, 446 U.S. 544, 555 (1980)).

96 *See Katz*, 389 U.S. at 352-53.

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

98 *Id.* at 404.

99 *Id.*

derived from property law, as the Court noted that there was no doubt "that such a physical intrusion would have been considered a 'search' within the [original] meaning of the Fourth Amendment."[100]

B. *Exceptions*

Various exceptions to the reasonable expectation of privacy requirement for constitutional protection have arisen throughout the span of Fourth Amendment jurisprudence. One notable exception, the abandonment principle, also derives from the Fourth Amendment's traditional focus on property law.[101] As articulated by the Third Circuit in *United States v. Harrison,* "a person can lose his reasonable expectation of privacy in his real property if he abandons it."[102] Whether the owner has abandoned his reasonable expectation of privacy in his property is a determination that "must be made from an objective viewpoint, and proof of intent to abandon must be established by clear and unequivocal evidence."[103] To determine this, the court will look to "the totality of the facts and circumstances."[104] The Supreme Court has extended this principle to trash left on the curb outside an individual's home in *California v. Greenwood*, holding that because trash is sufficiently exposed to public view, it cannot rise to the level of Fourth Amendment protection.[105] Discarded items will only rise to the level of constitutional protection if the manner in which those items were discarded nevertheless constitutes an expectation of privacy that society is prepared to accept as objectively reasonable.[106] With regard to seizures of physical DNA evidence abandoned by a perpetrator at the scene of a crime, scholars have explained that there is no need to afford any constitutional protection to such evidence, because where there is no suspect in mind, there is no Fourth Amendment right to protect.[107] State courts have also articulated this

100 *See id.* at 404-05.

101 John P. Ludington, Annotation, *Search and Seizure: What Constitutes Abandonment of Personal Property Within Rule that Search and Seizure of Abandoned Property is not Unreasonable—modern cases*, 40 A.L.R. 4th 381 (1985).

102 United States v. Harrison, 689 F.3d 301, 307 (3d Cir. 2012).

103 *Id.*

104 *Id.*

105 *See* California v. Greenwood, 486 U.S. 35, 40 (1988).

106 *Id*. at 39-40.

107 Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 Nw. L. REV. 857, 859 n.10 (2006).

standard. For example, in *State v. Athan*, police used a suspect's saliva left on an envelope to identify him.[108] There, the Supreme Court of Washington held that "[t]he analysis of DNA obtained without forcible compulsion and analyzed by the government for comparison to evidence found at a crime scene is not a search under the Fourth Amendment."[109]

Another prominent exception to the reasonable expectation of privacy requirement has been referred to as the third-party doctrine, which largely stems from inferences derived from the abandonment principle. The Supreme Court articulated this doctrine in *Smith v. Maryland* when it ruled that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[110] In *Carpenter v. United States,* the Supreme Court explained that "[t]he third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another."[111] However, the "diminished privacy interests" associated with the third-party doctrine do "not mean that the Fourth Amendment falls out of the picture entirely."[112] Instead, courts should consider "the nature of the particular documents sought to determine whether there is a legitimate expectation of privacy concerning their contents."[113]

IV. USER AGREEMENTS AND CURRENT FEDERAL REGULATIONS OF POPULAR GENEALOGY WEBSITES

The use of genealogy websites by the general public has skyrocketed in recent history. In fact, genealogy is currently the second most popular hobby in the United States, with genealogy websites being the second most frequently visited category of internet sites.[114] Despite genealogy websites' growing popularity, it is unclear whether individuals who willingly upload their DNA to these various services are fully

108 State v. Athan, 158 P.3d 27, 37 (Wash. 2007).

109 *Id.*

110 Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

111 Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

112 *Id.* (quoting Riley v. California, 573 U.S. 373, 392 (2014)).

113 *Id.* (quoting United States v. Miller, 425 U.S. 435, 442 (1976)).

114 Gregory Rodriguez, *How Genealogy Became Almost as Popular as Porn*, TIME (May 30, 2014), http://time.com/133811/how-genealogy-became-almost-as-popular-as-porn/. In this article, Time Magazine points out that the most popular hobby in the United States is gardening, and the most popular category of website visited is pornography. *Id.*

informed of how their information may be stored and used in the future.[115] For example, following the news surrounding the Golden State Killer case, GEDmatch was forced to release a statement specifying that users' genetic information, though primarily used to find distant relatives, *might* be used for other purposes, as it is not considered private under the third-party doctrine.[116]

Each genealogy website provides the public with information pertaining to their privacy policies and legal obligations with varying degrees of specificity and detail.[117] These measures largely are disclosed to indemnify the companies from legal action if personal user data is released to third parties.[118] Privacy policies also are disclosed to inform the public at large to which federal regulations these websites and the data stored therein are subject.[119] Each of the three genealogy websites discussed in this Comment vary in terms of the information provided in their privacy statements and terms of service in some respects, but there is some significant overlap with regard to federal statutes.

A. *23andMe*

23andMe, a popular genealogy website, says in its privacy security statement that the company "believes genetic information, as well as the systems put in place to protect it, deserve the highest level of security."[120] For this reason, 23andMe affirms that it will not give personal user data to any third party under any circumstances without explicit user consent, unless a valid warrant mandates the disclo-

---

115 CBSNEWS, *supra* note 40.

116 *See id.*

117 *See generally Privacy and Data Protection*, 23ANDME, https://www.23andme.com/privacy/ (last visited Oct. 18, 2019) [hereinafter *Privacy*, 23ANDME]; *see also Your Privacy*, ANCESTRY, https://www.ancestry.com/cs/legal/privacystatement (last visited Oct. 18, 2019) [hereinafter *Your Privacy*, ANCESTRY]; *see also Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last visited Jan. 21, 2020) [hereinafter *Privacy Policy*, GEDMATCH].

118 *See, e.g., Ancestry International Terms and Conditions*, ANCESTRY, https://www.ancestry.com/cs/legal/row-terms-and-conditions-en (last visited Nov. 21, 2019).

119 *E.g.*, Marcus Moretti & Michael Naughton, *Why Privacy Policies are so Inscrutable*, THE ATLANTIC (Sep. 4, 2014), https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/.

120 *Privacy*, 23ANDME, *supra* note 117.

sure.[121] 23andMe explicitly promises its users that it will not provide private user information to "law enforcement or regulatory authorities unless required by law to comply with a valid court order, subpoena, or search warrant for genetic or personal information."[122]

The average 23andMe user may find it difficult at first glance to find any relevant statutory constraints on legal liability for the website. In fact, users must first navigate through five separate web pages on 23andMe's website to find the company's "Guide for Law Enforcement" to understand the statutory underpinnings of 23andMe's privacy policy.[123] Although clearly not labeled to attract the attention of the typical user, this guide details to law enforcement all of the necessary steps they must take and the constraints they must overcome before the company will release private user data.[124] This page begins by stating that, "23andMe will only review inquiries as defined in 18 U.S.C. § 2703(c)(2) related to a valid trial, grand jury subpoena, warrant or order."[125] This subsection of the U.S. Code—under the general heading "Required disclosure of customer communications or records"[126]—requires the mandatory disclosure to law enforcement of certain records concerning electronic communications or remote computing services.[127] Under 18 U.S.C. § 2703(c)(2), providers of electronic communication or remote computing services must disclose the name, address, records of session times and durations, length of service, types of services utilized, subscriber number, and means and source of payment for the service to government entities upon a valid request.[128]

Additionally, the Guide for Law Enforcement states that 23andMe will consider releasing additional user information outside of the aforementioned statutory categories if they are prompted to do

---

121 *Privacy Highlights*, 23ANDME, https://www.23andme.com/about/privacy/ (last updated Sept. 30, 2019) [hereinafter *Privacy Highlights*, 23ANDME].

122 *Id.*

123 *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide/ (last visited Oct. 18, 2019). To reach this page, a user must navigate from the 23andMe homepage, to the "Privacy and Data Protection" page through a tab, then through a link on that page to the "Privacy Statement" page, then through a link on that page to the "Transparency Report" page, then finally through a link on that page to the "Guide for Law Enforcement."

124 *Id.*

125 *Id*.

126 18 U.S.C. § 2703 (2019).

127 18 U.S.C. § 2703(c) (2019).

128 *See* 18 U.S.C. § 2703(c)(2)(A)-(F) (2019).

so under a court order issued pursuant to 18 U.S.C. § 2703(d).[129] In relevant part, this subsection states that a court may issue such an order "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought are relevant and material to an ongoing criminal investigation."[130] The webpage then cites to 18 U.S.C. § 2703(f) to note that the company has never received a request to preserve information potentially relevant to legal proceedings pursuant to that subsection.[131] 18 U.S.C. § 2703(f) mandates that certain material requested under court order must be preserved for a ninety-day period.[132] Finally, 23andMe states that it will make every effort to notify a user if law enforcement has requested his personal data from the company, unless it is forbidden to do so by a Delayed Notice Order under 18 U.S.C. § 2705(b).[133] This statute states that a governmental entity, under certain circumstances, may apply for a "court order commanding a provider of electronic communications service[s] or remote computing service[s] . . . not to notify any other person of the existence of the warrant, subpoena, or court order [directed to them]."[134]

B. *Ancestry DNA*

The Ancestry DNA Guide for Law Enforcement contains the exact same protections and statutory constraints stated by 23andMe except that it does not mention 18 U.S.C. § 2703(f).[135] Therefore, under these two companies, users can expect that their personal data and information will be protected from third-party inquiry except under the extreme circumstance of a valid court order in criminal investigations. This language and statutory scheme is consistent with the Fourth Amendment's protection against unreasonable searches and seizures without a proper warrant issued "upon probable cause,

---

129 *23andMe Guide for Law Enforcement*, *supra* note 123.

130 18 U.S.C. § 2703(d) (2019).

131 *23andMe Guide for Law Enforcement*, *supra* note 123.

132 18 U.S.C. § 2703(f) (2019).

133 *23andMe Guide for Law Enforcement*, *supra* note 123.

134 18 U.S.C. § 2705(b) (2019).

135 *See Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/cs/legal/lawenforcement (last visited Oct. 18, 2019).

supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[136]

Ancestry DNA cites three governing privacy principles: transparency, simplicity, and control.[137] Ancestry DNA also ensures that there are "measures in place to protect against inappropriate access, loss, misuse, or alteration of personal information under [its] control," although it does not clarify what specific "measures" are in place.[138] Additionally, Ancestry DNA offers the assurance that if law enforcement compels it to disclose any user's personal information, its first priority will be to provide the user with advance notice so long as it is permissible under law.[139] Ancestry DNA further provides all visitors—whether they have signed up to use their service or not—with access to an annual transparency report disclosing all law enforcement requests for user data over the preceding year.[140] The 2018 report revealed that Ancestry DNA responded to seven out of a total of ten valid law enforcement requests in that year, all of which were related to investigations of credit card misuse or identity theft.[141] In sum, Ancestry DNA and 23andMe both prioritize user privacy, at least as far as they are legally permitted to do so.

C. *GEDmatch*

GEDmatch's privacy policy paints a wholly different picture of privacy than those articulated by both 23andMe and Ancestry DNA.[142] Unlike the more professional-looking 23andMe and Ancestry DNA websites, GEDmatch provides only a low-tech and minimalist user interface. Its terms of service and privacy policy pages were initially updated in May 2018, one month after the Golden State Killer case was solved.[143] Although much of the initial language of this page

---

136 U.S. CONST. amend. IV.

137 *Your Privacy*, ANCESTRY, *supra* note 117.

138 *Id.*

139 *Id.*

140 *Ancestry 2018 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency (last visited Jan 22, 2020).

141 *Compare id.*, *with Ancestry 2017 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency-2017 (last visited Jan. 20, 2020). The 2017 report revealed that Ancestry DNA responded to thirty-one out of a total thirty-four valid law enforcement requests in 2017, all of which were related to investigations of credit card misuse or identity theft.

142 *Privacy Policy*, GEDMATCH, *supra* note 117.

143 *Id.*

espouses a heightened importance in the protection of individual privacy, the true nature of the website is revealed under a heading titled "GEDmatch Purpose."[144] This section reads:

> GEDmatch exists to provide DNA and genealogy tools for comparison and research purposes. It is supported entirely by users, volunteers, and researchers. DNA and Genealogical research, by its very nature, requires the sharing of information. Because of that, users participating in this Site agree that their information will be shared with other users.

Therefore, unlike the typical legal protections enjoyed by users of more regulated websites, like 23andMe and Ancestry DNA, users of GEDmatch can expect that fellow users, any member of the general public, and even law enforcement may access the genetic information they have freely uploaded to the site.

GEDmatch, conversely, does not claim any statutory protection over its genetic content. GEDmatch brands itself largely as a public forum, rather than strictly a genealogy service.[145] Although it cites no statutory authority, GEDmatch does first establish that it "may disclose [users'] raw data, personal information, and/or genealogy data if it is necessary to comply with a legal obligation such as a subpoena or warrant."[146] The site even offers some possible alternative uses beyond simple genealogy research that users may access—including "familial searching by third parties such as law enforcement agencies to identify the perpetrator of a crime, or to identify remains."[147]

Further, GEDmatch's policy was recently updated on December 9, 2019, following the company's acquisition by Verogen, Inc.[148] The revised policy reflects a shift in the company's branding practices in the wake of the Golden State Killer investigation. Specifically, the policy now includes four options for users when uploading their DNA profiles to the website: "Private," "Public + opt-in," "Public + opt-out," and "Research."[149] Notably, the "Public + opt-out" option allows users to upload their DNA profiles for public comparison by

144 *Id.*
145 *Id.*
146 *Id.*
147 *Id.*
148 *Privacy Policy*, GEDMATCH, *supra* note 117.
149 *Id*.

other general users, but hides those profiles from users with profiles identified as having been uploaded "for Law Enforcement purposes."[150] Nevertheless, in this most recent revision, GEDmatch still fails to cite statutory authority for its policies, and retains portions of its policy notifying users of the inherent public nature of its product.

This policy stands in stark contrast to those outlined in the previous two websites. GEDmatch attempts to make it explicitly clear to users that the company is in no way responsible for breaches of information that is publicly accessible on its site. Under this scheme, the website functions largely like a social media platform, in which a majority of user data is voluntarily uploaded under the understanding that it can be freely accessed for any and all purposes.

V. THE COLORADO MODEL

In 2009, Colorado began to formally implement a policy of statewide familial DNA searching in criminal investigations, making it the first state in the U.S. to formally recognize familial DNA as an investigative resource.[151] Since then, Colorado's policy has become the gold standard for state familial DNA searching, with many states following suit in modeling their own policies after it.[152] Colorado has developed and proliferated its own familial DNA searching software, which is regularly tested and retested to ensure accuracy of results.[153] As of 2017, this software has been shared with local police departments in six additional states and has the capability of being fully downloaded and usable within an hour.[154] Users begin by uploading DNA profile data from the crime scene into the software's database.[155] The software then calculates ratios indicating the likelihood of familial relatedness between samples for all profiles in the system.[156] The software is also capable of organizing this data by familial relationship—such as parent-child, siblings, etc.—as well as race.[157] Finally,

---

150 *Id*.

151 MICHAEL B. FIELD, ET AL., NAT'L CRIMINAL REFERENCE SERV., STUDY OF FAMILIAL DNA SEARCHING POLICIES AND PRACTICES: CASE STUDY BRIEF SERIES 3 (2017), https://www.ncjrs.gov/pdffiles1/nij/grants/251081.pdf.

152 *Id.*

153 *Id*. at 5.

154 *Id.*

155 *Id.*

156 *Id*. at 6.

157 FIELD, ET AL., *supra* note 151, at 6.

based on the previously mentioned likelihood ratios, the software will export a table which displays the top selected profiles derived from comparison to the inputted DNA.[158]

There is no specific state legislation in Colorado that either explicitly prohibits or allows the use of familial DNA searches in criminal investigations, because the policy did not originate in the state legislature.[159] The policy of familial DNA searching was first proposed in the state by the Colorado Bureau of Investigations (CBI) and governed by the "CBI DNA Familial Search Policy."[160] After the CBI developed this policy, the state Attorney General approved and put it into effect state-wide in October of 2009.[161] The CBI policy defines familial DNA searching as "a deliberate search for biologically-related relatives of a contributor of an evidentiary profile conducted with specialized (non-CODIS) software designed for this purpose."[162] Because of the obvious privacy concerns and implications the new policy would surely elicit, the CBI was careful to implement incredibly specific and detailed procedures for state law enforcement to follow with each initial familial DNA search request.[163]

First, the request must originate from one of two sources: (1) "analysts within the [CBI or Denver PD Crime] lab identify cases they think are good candidates for [familial DNA searching] and go to their lab director requesting permission;" or (2) directly from a law enforcement agency.[164] Requests under either circumstance must meet a number of strict criteria.[165] First, not only must the case have already undergone a CODIS search with no results, but the lab must also be confident that the law enforcement agency has fully exhausted *all* alternative investigative leads.[166] Second, the request is subject to the professional opinion of the lab staff before familial DNA searching can be approved.[167] In this determination, lab staff will consider a number of factors, including "public safety implications, the age of the case, and the types of evidence available" to ensure that the case is

158 *Id.*
159 *Id.*
160 *Id.*
161 *Id.*
162 *Id*.
163 FIELD, ET AL., *supra* note 151, at 7-9.
164 *Id*. at 7.
165 *Id.*
166 *Id.*
167 *Id.*

sufficiently compelling to justify the significant monetary and time expenditure of familial DNA search analysis.[168] In circumstances where the request comes directly from law enforcement, lab staff will meet with the officers to fully inform them of the familial DNA search process.[169] After all relevant information has been shared with the officers, they are required to sign a form indicating their understanding of the procedure and relevant factors surrounding it before any analysis can commence.[170] This form also indicates a commitment from the officers that if a match or lead is discovered through familial DNA searching, officers must continue their investigation of the case so as to not have wasted lab resources.[171] This penultimate step in the process has been cited by both law enforcement entities as well as the Denver PD Crime Lab as one of the most integral parts of the request policy—the formal agreement between parties to take and maintain responsibility of the case so that neither party feels as though their time, finances, or energy is wasted.[172] Finally, the prosecutor of each case will be added to the formal familial DNA searching process to ensure the proper follow-up of any leads produced, continuing the chain of responsibility.[173] Ultimately, the crime lab's director makes the final decision of whether a familial DNA search will be conducted on any given case.[174]

ANALYSIS

This section sets forth a model framework based on the Colorado Model which, if implemented through federal legislation, would provide a uniform request and analysis process for investigative use of familial DNA searching that would afford heightened protections of the privacy rights of individuals. Specifically, this Part will first provide a comprehensive analysis of the Fourth Amendment implications in the Golden State Killer case under current legal standards. Then, this Part will apply these same facts to the processes and procedures of the Colorado Model. Finally, this Part will discuss the differing out-

168 *Id.*
169 FIELD, ET AL., *supra* note 151, at 7.
170 *Id*.
171 *Id.*
172 *Id.*
173 *Id.*
174 *Id.*

comes of these two methods and ultimately conclude that the Colorado Model provides for a more streamlined, thorough, and uniform request system. Federal implementation of the Colorado Model would, therefore, provide for greater constitutional privacy protections for individuals while also improving upon the current process of familial DNA searching.

I. FOURTH AMENDMENT IMPLICATIONS IN THE GOLDEN STATE KILLER INVESTIGATION & PENDING TRIAL

Under the current regulatory scheme surrounding the Fourth Amendment, it is unlikely that any significant constitutional impediments will arise in Joseph DeAngelo's upcoming trial. Assuming, *arguendo*, DeAngelo does assert a constitutional claim, the court will likely begin its analysis by determining whether DeAngelo had a reasonable expectation of privacy in the DNA he shed at the initial crime scene or the more recent DNA he shed on his car door handle and in his trash.[175] Under the abandonment standards articulated in *Greenwood* and *Athan*, the inquiry would likely end at this preliminary juncture.[176] Under *Athan*, as well as under conventional wisdom in police investigations, DeAngelo has no reasonable expectation of privacy in the DNA left in the commission of his original crimes and collected during the course of routine police investigation.[177] Further, in addition to the abandoned DNA later collected by police from a tissue discarded in his trash, the DNA retrieved from the handle of his car—parked in a public parking lot—would not survive Fourth Amendment scrutiny because both were discarded and subject to public view, therefore constituting a lower manifest privacy interest.[178] Because all three of these samples do not meet the objective reasonableness standard from the perspective of society, DeAngelo could have no reasonable expectation of privacy that would afford him Fourth Amendment protection.[179]

---

175 *See* California v. Ciraolo, 476 U.S. 207, 211 (1986) (citing Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

176 *See* California v. Greenwood, 486 U.S. 35, 39-40 (1988); State v. Athan, 158 P.3d 27, 37 (Wash. 2007).

177 *Athan*, 158 P.3d at 37.

178 *Greenwood*, 486 U.S. at 39-40; United States v. Harrison, 689 F.3d 301, 307 (3d Cir. 2012).

179 *Greenwood*, 486 U.S. at 39-40.

However, it is also important to view this constitutional question from the perspective of the innocent distant family member whose DNA led to the capture and arrest of the perpetrator. This inquiry is much murkier in the Fourth Amendment context. Assuredly, if the DNA had been uploaded to one of the more secure websites, such as 23andMe or Ancestry DNA, the question of reasonableness of the objective expectation of privacy would be more clear based on the safeguards promised in their privacy statements.[180] However, given the objectively lower standard articulated by GEDmatch, there is a significant likelihood that a court would find no Fourth Amendment violation resulting from the police action here.[181] Fourth Amendment protection extends to intrusions of constitutionally protected areas unless the technology used to conduct the search was in general public use.[182] GEDmatch is well within public use as it is marketed as an open-source database in which "information will be shared with other users."[183] The website's very nature facilitates public use, and no user who willingly shares personal data with such a public forum can reasonably expect such data to remain confidential. GEDmatch makes no secret that users may find numerous other uses for the data uploaded to the website and therefore openly employs a "participate at your own risk" policy. Under current Fourth Amendment precedent, there is likely no chance that a court would uphold a constitutional claim purported by the willing GEDmatch user in this case.

II. APPLICATION OF THE COLORADO MODEL TO THE GOLDEN STATE KILLER INVESTIGATION

Unlike the application of Fourth Amendment analysis, the Colorado standard, if applied strictly, could produce vastly different results in the DeAngelo case. Under the Colorado framework, the request for familial DNA searching in this case would come from the policy's second stated source category—directly from law enforcement.[184] Under a federally mandated Colorado-style policy, California state investigators handling the Golden State Killer case could submit a for-

180 *Ancestry Guide for Law Enforcement*, *supra* note 135; *Privacy*, 23ANDME, *supra* note 117.

181 *See Privacy Policy*, GEDMATCH, *supra* note 117.

182 Kyllo v. United States, 533 U.S. 27, 34 (2011).

183 *Privacy Policy*, GEDMATCH, *supra* note 117.

184 FIELD, ET AL., *supra* note 151.

mal request for familial DNA search analysis of the DNA retrieved from the crime scene. Then, this request would be tested under the strict Colorado criteria. First, law enforcement officials must verify to the crime lab that the DNA had already been put through a CODIS search and yielded no results.[185] As previously discussed, the DNA profile yielded by police using the crime scene DNA left behind by the Golden State Killer was not a match with any of the known felons in the CODIS database.[186] Next, the crime lab would determine whether law enforcement had exhausted all other possible leads.[187] Here, it is clear that after nearly forty years of deliberate investigation, all possible leads had been thoroughly examined. After passing this initial inquiry, the request would then be subject to the professional evaluation of the crime lab analysts.[188] The Golden State Killer case, having gone cold after a period of nearly forty years, is clearly of a significant public interest in terms of safety implications.[189] Under a cost-benefit analysis of the necessity for familial DNA searching in this case, any rational crime lab would undoubtedly move forward, given the sheer amount of lives lost and compassion for the families still suffering. Thereafter, the crime lab analysts would meet with representatives from the California law enforcement agencies who submitted the formal request to fully apprise them of the nature of familial DNA searching and to garner a contractual obligation to continue the investigation if results are successfully yielded.[190] Finally, if a prosecutor had been assigned at that point, she too would be added to this agreement so that all parties share in accountability for the resources expended.[191] Under this scenario, the same results would be produced as would be under the current framework. Even so, the positive implications stemming from the strict scrutiny and accountability standards employed in the Colorado model cannot be diminished. Under these standards, there is an assurance of thoroughness, attention to detail, and accountability, thus ensuring the protection of the rights of all parties involved to the fullest extent possible.

---

185 *Id.*

186 *See* MCNAMARA, *supra* note 8, at 302; *see also* Wamsley, *supra* note 3.

187 FIELD, ET AL., *supra* note 151.

188 *Id.*

189 *Id.*

190 *Id.*

191 *Id.*

III. THE IMPERATIVE NEED FOR COMPREHENSIVE FEDERAL REGULATION

It is clear from this analysis that no current federal regulations effectively protect the privacy rights of individuals with regard to familial DNA searching in the same comprehensive manner as the Colorado Model. As demonstrated, a simple Fourth Amendment analysis will often fail to extend to such specific instances as those presented here, so long as the DNA collected and tested is publicly available. Additionally, the statutes cited by both 23andMe and Ancestry DNA serve as insufficient guidance for the intricacies involved in DNA retrieval and analysis. The federal legislation contained in 18 U.S.C. § 2703 too broadly covers inquiries with regard to "required disclosures of customer communications or records" in a "remote computing" setting.[192] This incredibly wide-sweeping language is intended to touch upon a variety of web-based communications and does not inherently evoke any cognizant relation for genealogy websites or familial DNA searching. However, the sheer lack of federal guidance or legislation is not surprising given the relative recency and popularity of such services. As the court stated in *United States v. Jones*, "dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes."[193] With this change in popular attitude must come a change in law.

Specific federal legislation aimed at familial DNA searching would provide a uniformity in the request and analysis process that affords heightened protections of the privacy rights of individuals. Instead of allowing for variances in state-implemented policies, cohesive federal regulations would work directly with existing technology, such as CODIS, to produce the most efficient and accurate results. Federal implementation of the Colorado Model would accomplish these objectives. As previously stated, the Colorado familial DNA searching policy has served as a pioneer for other state policies across the country.[194] The FBI could easily implement the process of carrying out this policy in the same way the CBI conducts it within Colorado. Using the highly sophisticated crime labs already in regular use

192 18 U.S.C. § 2703(c) (2019).

193 United States v. Jones, 565 U.S. 400, 427 (2012).

194 FIELD, ET AL., *supra* note 151.

within the FBI, analysts could begin implementing the Colorado Model's strict scrutiny standards to requests received from all over the country immediately upon adoption. These standards, applied at the federal level, would more closely align with the goals and purposes of the Fourth Amendment, and would provide the necessary vetting and consideration needed before permitting the encroachment upon those rights. In addition to this enhanced Fourth Amendment protection, this policy would produce more efficient and accurate results through familial DNA searching, allowing federal agents to successfully solve more crimes like the Golden State Killer case.

CONCLUSION

The right to privacy is an integral tenant of the freedoms guaranteed to American citizens in the Constitution. However, the current legal restrictions pertaining to familial DNA searching through genealogy websites provide for little substantive protection of this right. Under the current framework, virtually all law enforcement requests for familial DNA data will survive a constitutional challenge in court, as most samples are submitted voluntarily, and police necessity typically takes precedence over arbitrary and attenuated privacy claims in voluntarily uploaded DNA profiles. Additionally, the current standard does not require any formal process by which police must exhaust other options, nor does it require a cost-benefit analysis of privacy concerns. Therefore, the present system places police necessity—arbitrary or otherwise—above the individual privacy rights of American citizens. The Colorado Model, conversely, maintains a viable option for police access for familial DNA data, while keeping in mind the sanctity of an individual's right to privacy. By requiring proof of police exhaustion of alternative methods, as well as a thorough interest-balancing analysis, this model would lead to greater police accountability while providing a clear and formulaic process for familial DNA requests. Federal implementation of the Colorado Model would provide a clear and uniform federal standard for familial DNA searching. This proposal would provide a viable solution to the inherent privacy concerns that arise from the growing use of genealogy websites for investigatory purposes. A solution such as this will only become more necessary as public genealogy technology continues to expand. Otherwise, an individual's right to privacy as it currently exists will diminish as it is forced to adapt to police demands.