AN INVASION OF PRIVACY: GENETIC TESTING IN AN AGE OF UNLIMITED ACCESS

Najla Hasic

"[T]he history of the criminal law proves that tolerance of shortcut methods in law enforcement impairs its enduring effectiveness."[1]

I. INTRODUCTION

In 2018, the case of a high-profile serial killer captured the attention of people throughout the United States.[2] Yet, it is not the killer that many are interested in, but rather the manner in which he was identified. The Golden State Killer terrorized the suburbs of Sacramento between 1976 and 1986.[3] Police suspect he was responsible for twelve murders and more than fifty rapes.[4]

Deoxyribonucleic Acid (DNA) was left at multiple crime scenes, but criminal DNA databases produced no hits that could identify the perpetrator.[5] In 2016, Sacramento County District Attorney helped start a high-profile campaign to find the Golden State Killer.[6] Police used the DNA recovered from the crime scene to find the killer's great-great-great grandparents, who lived in the early 1800s.[7] Discovery of these distant relatives was made possible by GEDmatch, a direct-to-consumer (DTC) genetic testing company, which enables individuals to look up information about their genetic background.[8] After carefully combing through each family member's DNA, the police ultimately identified seventy-two-year-old Joseph James DeAngelo, Jr. as a likely match for the DNA found at the crime scenes.[9] Once police pinpointed their new suspect, they placed him under surveillance and started collecting samples of his DNA without his knowledge.[10] DeAngelo lived free of suspicion for over thirty years, until the DNA of a five-times-removed relative connected him to over sixty crime scenes.

---

1 Miller v. United States, 357 U.S. 301, 313 (1958).

2 Laurel Wamsley, *After Arrest of Suspected Golden State Killer, Details of His Life Emerge*, NATIONAL PUBLIC RADIO (Apr. 26, 2018), https://www.npr.org/sections/thetwo-way/2018/04/26/606060349/after-arrest-of-suspected-golden-state-killer-details-of-his-life-emerge.

3 *Id.*

4 Avi Selk, *The Most Disturbing Parts of the 171-page Warrant for the Golden State Killer Suspect*, WASHINGTON POST (June 2, 2018), https://www.washingtonpost.com/news/post-nation/wp/2018/06/02/the-most-disturbing-parts-of-the-171-page-warrants-for-the-golden-state-killer-suspect/.

5 TJ Ortenzi, *Hunt for Golden State Killer Led Detectives to Hobby Lobby for DNA Sample*, WASHINGTON POST (June 2, 2018), https://www.washingtonpost.com/news/post-nation/wp/2018/06/02/hunt-for-golden-state-killer-led-detectives-to-hobby-lobby-for-dna-sample/.

6 Wamsley, *supra* note 2.

7 Justin Jouvenal, *Search of Family Trees Led to Serial-Killing Suspect*, WASHINGTON POST (May 1, 2018), https://search-proquest-com.proxy.lib.siu.edu/docview/2032676809?accountid=13864.

8 *Id.*

9 *Id.*

10 Ortenzi, *supra* note 5.

Due to the many actors involved, this new method of solving cold cases presents a very nuanced issue. This Note discusses how privacy rights are implicated when DTC genetic testing companies disclose an individual's genetic information to law enforcement officers—who then use that data to implicate an individual's family members. Additionally, this Note explains how the current landscape of judicial and legislative privacy protections are inadequate in this instance and offers a statutory solution as the proper method of addressing genetic privacy.

Part II of this Note discusses DNA, what it is and how it is used and tested by both state and private actors. It also provides a brief history of the Fourth Amendment with a specific focus on its application in jurisprudence as technology advances and privacy rights diminish. Finally, an overview of current statutory law related to general and genetic privacy rights as passed by Congress and individual states is offered. Part III analyzes the issues with attempting reconcile current Supreme Court precedent interpreting the language of the Fourth Amendment to account for all of the complexities involved when dealing with genetic privacy. Part IV offers a statutory solution that will protect genetic privacy by proposing a new federal law that will (1) Require DTC ancestry and genealogy companies to adopt an automatic "opt-out" policy for consumers; and (2) Prohibit DTC genealogy and ancestry companies from sharing familial information with law enforcement agencies. The proposed statute will attempt to balance current Supreme Court precedent interpreting the Fourth Amendment, public policy interests in allowing law enforcement to solve crimes, and the need for rigid protection of genetic information in an age of incessantly advancing technology.

II. BACKGROUND

The trend of using DNA as evidence in criminal cases began in the mid-1980s and since then has been developed in fascinating ways.[11] The Supreme Court's approval of DNA collection and evidence has led to national and state databases containing DNA profiles of individuals convicted of some crimes.[12] These databases have made it easier for law enforcement officials

---

[11] NATIONAL RESEARCH COUNCIL, DNA TECHNOLOGY IN FORENSIC SCIENCE VII (THE NATIONAL ACADEMIES PRESS) (1992).

[12] *Id.* at 142-143; *see also generally* Maryland v. King, 569 U.S. 435 (2013) (holding that the Fourth Amendment allows states to collect and analyze DNA from people arrested, but not convicted of serious crimes); Vernonia School Dist. 47J v. Acton, 515 U.S. 646 (1995) (holding students in public schools have a reduced expectation of privacy and may be required to undergo vaccinations or medical exams in order to protect the student body. Student athletes have an even more reduced expectation of privacy and can be required to submit a urine samples from drug testing); *and* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602 (1989) (holding drug testing of railway employees on the grounds that employees nationwide had been using drugs was held constitutional).

to link crimes to perpetrators.[13] Nevertheless, law enforcement officers pushed Constitutional limits by using familial matches to connect individuals to crimes, and now they are using private databases owned by private companies to do the same, raising serious privacy concerns.[14] Familial matching itself raises privacy concerns, and those concerns are exacerbated when information is pulled from private consumer genealogy databases, without thought of criminal implication.

In order to fully understand how law enforcement's unauthorized use of data provided to DTC companies implicates genetic privacy rights, it is essential to understand what DNA is, how it is tested, and finally, how it is currently being used to aid criminal investigation and ancestral research. The following first provides an overview of the mechanics and prevalence of DNA to aid readers in understanding why unauthorized uses invade the privacy of an individual as well as their family members. Then, a summary of relevant Fourth Amendment principles as interpreted by the Supreme Court is offered, as well as current federal and state statutory law related to both general and genetic privacy rights in the United States.

A. DNA: What It Is and How It Is Shared

DNA is a molecule that contains the biological instructions that make up an individual.[15] In humans, DNA molecules are tightly packaged into forty-six chromosomes, which are passed from adult organisms to their offspring during reproduction.[16] Each parent passes on twenty-two chromosomes and one sex chromosome, which blend together to make the full genome.[17] Thus, each individual's genome is comprised of one half of the mother's chromosomes and one half of the father's. The first twenty-two chromosome pairs are numbered chronologically one through twenty-two and the last pair consists of two sex determining chromosomes labeled either XX or XY.[18]

---

13 *See generally* Howard Safir, *DNA Technology as an Effective Tool in Reducing Crime*, FORENSIC MAGAZINE (Oct. 1, 2007), https://www.forensicmag.com/article/2007/10/dna-technology-effective-tool-reducing-crime.

14 Kristen V. Brown, *DNA Detectives are Searching for Killers in Your Family Tree*, BLOOMBERG LAW (June 14, 2018), https://www.bloomberg.com/news/features/2018-06-14/dna-detectives-are-searching-for-killers-in-your-family-tree.

15 *Deoxyribonucleic Acid (DNA) Fact Sheet*, NATIONAL HUMAN GENOME RESEARCH INSTITUTE, https://www.genome.gov/about-genomics/fact-sheets/Deoxyribonucleic-Acid-Fact-Sheet (last updated Nov. 13, 2019 [hereinafter *DNA Fact Sheet*].

16 The mother passes an X sex chromosome and the father can pass either an X or Y. *See id.*

17 Amanda Pattock, *It's All Relative: Familial DNA Testing and the Fourth Amendment*, 12 MINN. J.L. SCI. & TECH. 851, 854 (2011).

18 *Id.* An XX pair is female and XY is male.

Within chromosomes are billions of base pairs of DNA.[19] Base pairs are created by pairing two out of the four nucleotides.[20] The two nucleotide pairs are adenine (A) and thymine (T), and guanine (G) and cytosine (C).[21] The process of nucleotide pairs forming an order (A-T, T-A, G-C, and C-G) is called genetic sequencing.[22] Genetic sequencing creates the genes that determine looks and other traits such as hair and eye color.[23]

Within the genome there are both coding and non-coding genes.[24] The non-coding regions encompass repeated units of DNA that vary in length.[25] The particular repeated unit that aids law enforcement in identification is called a short tandem repeat (STR).[26] The number of repeats within an STR is called an allele.[27] Each allele has a fixed locus, or location, on a particular chromosome.[28] The loci allow for alleles to act as genetic markers, distinguishing individuals from one another and serving as a means for identification.[29]

B. Genetic Testing and Storage

Since the discovery of polymerase chain reaction (PCR)—the process by which DNA is copied—DNA testing has advanced significantly.[30] PCR uses the enzyme polymerase to replicate DNA regions allowing for a small number of DNA molecules to be increased up to billions.[31] Once DNA has been replicated enough to form a proper testing sample, analysts can use STR technology, Y-chromosome (Y-STR) analysis technology, or mitochondrial DNA (mtDNA) analysis technology to identify patterns and variations.[32]

As previously mentioned, STR technology evaluates specific loci found on nuclear DNA.[33] Y-STR technology, on the other hand, can only detect genetic markers on the Y chromosome, and thus, can only target the male fraction of a biological sample (as females lack a Y chromosome).[34] MtDNA

---

19 *Id.*
20 *Id.*
21 *DNA Fact Sheet*, *supra* note 15.
22 *Id.*
23 *Id.*
24 Pattock, *supra* note 17, at 854.
25 *Id.*
26 National Institute of Justice, *DNA Evidence: Basics of Analyzing*, DEPARTMENT OF JUSTICE OFFICE OF JUSTICE PROGRAMS (Aug. 8, 2012), https://nij.gov/topics/forensics/evidence/dna/basics/pages/analyzing.aspx.
27 Pattock, *supra* note 17, at 855.
28 *Id.*
29 *Id.*
30 National Institute of Justice, *supra* note 26.
31 *Id.*
32 *Id.*
33 *Id.*
34 *Id.*

analysis enables forensic laboratories to develop DNA profiles from evidence that is unsuitable for STR analysis.[35] This is because mtDNA technology analyzes mitochondria, which is found in the fluid that surrounds the nucleus of a cell.[36] However, mtDNA is only passed down by a mother to her offspring; therefore, testing of mtDNA will only reveal an individual's maternal bloodline,[37] although it will also reveal medical information about the individual which is stored in the coding regions of mtDNA.[38]

When DNA of an unknown individual is submitted for testing against a database, the results will be considered either a match or an exclusion.[39] A match occurs if the results are consistent with the results from a known individual within the database.[40] This means that all of the loci are the same between the two samples. That individual is then considered a possible source of the DNA found in the unidentified sample. Results that partially match with an existing DNA profile are considered exclusions.[41] Exclusions can be used to aid further investigation into the excluded individual's family members. Law enforcement has been using this method of identification to solve cases since the mid-nineties.[42]

1. The Government's Use of Our Genetic Information

Forensic DNA analysis was first used in 1987 to catch a rapist and murderer, Colin Pitchfork, and to exonerate an innocent, Richard Buckland.[43] In 1990, the Federal Bureau of Investigation (FBI) created the Combined DNA Index System (CODIS) database to standardize collection and storage of DNA profiles taken from missing persons, convicted felons, and forensic evidence found at crime scenes.[44] Four years later, Congress passed the DNA Identification Act which created the national program, the National DNA Index System (NDIS).[45] Shortly after, the DNA Analysis Backlog Elimination Act was passed authorizing the Attorney General to make grants

---

35 *Id.*

36 *Id.*

37 *Id*.

38 National Institute of Health, *Mitochondrial DNA*, U.S. NATIONAL LIBRARY OF MEDICINE (Jan. 7, 2020), https://ghr.nlm.nih.gov/mitochondrial-dna#.

39 National Institute of Justice, *supra* note 26.

40 *Id.*

41 *Id.*

42 Pattock, *supra* note 17, at 856.

43 Suzanne Elvidge, *Forensic Cases: Colin Pitchfork, First Exoneration Through DNA*, EXPLORE FORENSICS (July 18, 2016), http://www.exploreforensics.co.uk/forenisc-cases-colin-pitchfork-first-exoneration-through-dna.html.

44 Pattock, *supra* note 17, at 856.

45 34 U.S.C. § 12592 (transferred from 42 U.S.C. § 14132).

to states for the use of CODIS.[46] Over the years, the list of qualifying crimes for entry into the databases has increased and some states allow, and even require, collection of genetic information from arrestees and misdemeanants. Additionally, victims, excluded suspects, and lab workers' DNA is also kept in local databases.[47] As of September 2019, the National DNA database contained over fourteen million offender profiles, over three million arrestee profiles, and almost one million forensic profiles.[48] Since its implementation, CODIS has assisted almost half a million investigations.[49]

There are three primary database systems that comprise CODIS: the Local DNA Index System (LDIS), where the DNA profile originates; the State DNA Index System (SDIS), which allows for DNA information sharing among laboratories within the states; and the National DNA Index System (NDIS), which allows for the comparison of DNA information among the states.[50] The interworking of the three systems allows a DNA profile from one crime scene to be linked to other crime scenes and/or DNA profiles obtained from individuals convicted of crimes in other jurisdictions.[51]

Pursuant to the DNA Identification Act, states may participate in the National DNA Index so long as the participating laboratories are accredited criminal justice agencies, comply with the Quality Assurance Standards issued by the FBI, undergo external audits every two years, and abide by federal law regarding limited access to DNA samples and records.[52]

Federal law allows disclosure of DNA profiles only for purposes of law enforcement identification, to aid in judicial proceedings, to a defendant for criminal defense purposes, or for a population statistics database (so long as personally identifiable information is removed).[53] If a state does not comply with the DNA Identification Act, the violating state or laboratory may lose access privileges to the index.[54]

An officer conducting a search in CODIS has the option of choosing a high, medium, or low stringency search.[55] A high stringency search will match all twenty alleles from the two samples being compared, medium stringency is specifically dictated by the searcher, and low stringency

---

46 DNA Backlog Elimination Act of 2000, Pub. L. No. 106-546, (codified as amended in scattered sections of 42 U.S.C. §§ 13701, 14135).

47 Elizabeth Pike, *Securing Sequences: Ensuring Adequate Protections for Genetic Samples in the Age of Big Data*, 37 CARDOZO L. REV. 1977, 1997 (July 2016).

48 *CODIS-NDIS Statistics*, FEDERAL BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics (last visited July 6, 2019).

49 *Id.*

50 John M. Butler, *DNA Databases: Uses and Issues*, ADVANCED TOPICS IN FORENSIC DNA TYPING: METHODOLOGY 213, 213 (2012).

51 *Id.*

52 34 U.S.C. § 12592 (b)(2).

53 *Id.* at (b)(3).

54 *Id.* at (c).

55 Pattock, *supra* note 17, at 857-58.

searches will match at least one allele.[56] The results of low and medium stringency searches are called partial matches—which make familial searching possible.[57]

It is important to note that forensic DNA testing is not used to identify a specific individual per se, but rather to compare whether one DNA sample came from the same individual as another DNA sample.[58] When running a search in the database, it is likely to return matches of persons not related at all.[59] This is possible because all human genomes host the same types of genes, but the genes themselves may differ slightly, which accounts for the fact that all humans are extremely alike and yet utterly unique. After conducting a lower stringency search, the individuals whose DNA profiles have partial matches are excluded as suspects but are then used as an investigation tool to find the matching relative.[60]

Although federal law clearly establishes the parameters for how, when, and why CODIS is used, federal law is silent on the issue of "familial searching." In effect, familial searching uses DNA databases to find relatives who may be the source of the DNA found at the crime scene. The search can be done in two different ways. The first is when the searcher is running a degraded sample of DNA against the index, and the second is when running a full sample which returns DNA profiles with only some commonalities.[61] These hits are then used as starting points in the investigation.[62]

Currently, federal law enforcement agencies do not conduct familial searching and it is expressly prohibited in Maryland and Washington D.C.[63] Familial searching has been rejected at the federal level due to concerns regarding efficiency, misidentification, and difficulty in establishing a threshold ranking for review of a database of over ten million records when additional filters (such as geography and Y-STR testing) may not be available.[64]

Additionally, law enforcement will also seek out "abandoned" DNA from things left behind by a suspect. Law enforcement can obtain DNA samples from "bloodstains, semen stains, bones, teeth, hair, saliva, urine, feces, fingernail debris, muscle tissue, cigarette butts, postage stamps,

---

56 *Id*. at 858.
57 *Id*.
58 *Id*. at 854-55.
59 Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 298 (2010).
60 *Id*. at 297-98.
61 Pattock, *supra* note 17, at 858.
62 *Id*.
63 *Combined DNA Index System (CODIS)*, FEDERAL BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis, (last visited Feb. 16, 2020).
64 *Id*.

dandruff, and, ironically, fingerprints."[65] For example, during the Golden State Killer investigation, law enforcement obtained a discarded tissue from DeAngelo's trash can and fingerprints from the handle of his car door, tested it against the crime scene DNA evidence, and found that the two samples matched.[66] There are essentially no limits—legislative or judicial—on the collection of abandoned DNA.[67] Abandoned DNA has also allowed the government to toll statutes of limitations by filing charges against unidentified suspects by way of "John Doe warrants" and "DNA profile indictments."[68] These warrants and indictments are filed against DNA found at the crime scene and then placed into the CODIS database. Prosecutors will then wait for a "hit" matching the crime scene DNA to an individual.[69] The Supreme Court has held that an individual cannot have a legitimate expectation of privacy in something abandoned or shared with a third party, rendering such police practices constitutional.[70]

2. Private Direct-to-Consumer Companies' Uses of Genetic Information

Genealogy research has had a following in the United States since the early nineteenth century.[71] It has been done out of curiosity regarding one's history, to increase familiarity with the family tree, to reveal medical issues or genetic traits, and for the resolution of legal and financial matters, such as probate.[72]

Digital technology and the Internet have provided quick, easy, and convenient access to the tools that may provide those answers. Commercial DNA companies like Ancestry.com and 23andMe quickly emerged and took over the market. The home testing kits supplied by these companies only require consumers to mail in a cheek-scraping (buccal swab) or a cup of

---

65 Albert E. Scherr, *Genetic Privacy and the Fourth Amendment: Unregulated Surreptitious DNA Harvesting*, 47 GA. L. REV. 445, 450-51 (2013) (citations omitted).

66 Breeanna Hare & Christo Taoushiani, *What We Know About the Golden State Killer Case, One Year After a Suspect Was Arrested*, CNN (Apr. 24, 2019), https://www.cnn.com/2019/04/24/us/golden-state-killer-one-year-later/index.html.

67 Elizabeth Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. UNIV. L. REV. 857, 862 (2006).

68 Meagan Flynn, *The Culprit's Name Remains Unknown. But He Licked a Stamp, and Now His DNA Stands Indicted*, WASHINGTON POST (Oct. 17, 2018).

69 *Id.*

70 California v. Greenwood, 486 U.S. 35, 43-44 (1988) (holding that the Fourth Amendment does not prohibit warrantless searches and seizures of garbage left for collection outside the curtilage of a home); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

71 François Weil, *John Farmer and the Making of American Genealogy*, 80 NEW ENG. Q. 408, 416 (Sept. 2007).

72 National Institute of Health, *What is Direct-to-Consumer Genetic Testing?*, U.S. NATIONAL LIBRARY OF MEDICINE (Jan. 7, 2020), https://ghr.nlm.nih.gov/primer/dtcgenetictesting/directtoconsumer.

saliva.[73] Analysts then perform autosomal DNA tests, which look at specific locations of the individual's genome to find ancestral genealogical relationships or estimate the ethnic mixture of the individual.[74] In 2017, the genetic genealogy testing market was comprised of over twelve million customers.[75] The number and kind of online services available to individuals is growing—some help individuals learn their ancestry and others are able to generate health reports interpreting genetic data.[76]

GEDmatch is a DTC company of particular relevance. It is considered an *open data personal genomics database*. What this means is that the website allows consumers to upload their autosomal DNA test data from any commercial DNA company and then GEDmatch identifies potential relatives who have also uploaded their own profile.[77] By May of 2018, 929,000 genetic profiles existed in the GEDmatch database alone.[78] Considering the vast amount of genetic information already existing in GEDmatch's database and already shared among researchers, it is imperative Congress enact legislation to help protect privacy rights for those individuals and their families. Furthermore, the ways in which the "now-public" genetic information can be used in the future remains unexplored territory.

The Terms of Service and Privacy Policy was first revised by GEDmatch in May of 2018, after the Golden State Killer was caught, to include a section explaining that once an individual has uploaded their DNA it may be used for other purposes.[79] One of the new purposes listed was "familial searching by third parties such as law enforcement agencies to identify the perpetrator of a crime, or to identify remains."[80] Eric Heath, the Chief Privacy Officer for Ancestry.com, expressed concerns over the decision not to challenge the search warrant in the interests of their user's privacy made by GEDmatch.[81] More recently, GEDmatch again updated its terms of service to state that consumers automatically "opt out" of sharing information with law enforcement and, those who want their DNA shared

---

73 National Institute of Health, *How is Direct-to-Consumer Genetic Testing Done?*, U.S. NATIONAL LIBRARY OF MEDICINE (Jan. 7, 2020), https://ghr.nlm.nih.gov/primer/dtcgeneticstesting/dtcprocess.

74 *Id.*

75 Christi Guerrini et al., *Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique*, PLOS BIOLOGY 1, 6 (Oct. 2, 2018).

76 *Id.*

77 *Terms of Service and Privacy Policy*, *GEDMATCH*, *GEDmatch.com/tos.htm [hereinafter GEDmatch* Policy].

78 Kristen V. Brown, *DNA Website Had Unwitting Role in Golden State Manhunt*, BLOOMBERG (May 29, 2018), https://www.bloomberg.com/news/articles/2018-05-29/killer-app-dna-site-had-unwitting-role-in-golden-state-manhunt.

79 *GEDmatch Policy*, *supra* note 77.

80 *Id.*

81 Eric Heath, *Your Privacy is Our Top Priority*, ANCESTRY BLOG (Nov. 8, 2019), https://blogs.ancestry.com/ancestry/2019/11/08/your-privacy-is-our-top-priority/.

may opt back in.[82] This change reduced the number of samples available from 1.2 million to 140,000,[83] highlighting the public's disapproval of the new investigative technique.

Current privacy protections come in two forms: judicial (by way of the Fourth Amendment, for which you must have a legitimate expectation of privacy) and legislative (which has, thus far, only protected identifiable health information). Neither of these two types of existing privacy protections have been extended to cover genetic information held by DTC companies as they apply to family members of those consumers who utilized the company's services.

3. Public Meets Private

The fact that GEDmatch is a free, open data website means that anyone with an e-mail address has the ability to sign up, submit DNA information, and find relatives—including law enforcement officials. As of May 2018, Parabon NanoLabs, a private forensics company, has been working in cooperation with American law enforcement to solve unsolved crimes, implicating additional privacy concerns.[84] Parabon NanoLabs uploads DNA evidence from crime scenes to GEDmatch and then uses that information to identify perpetrators or relatives who could then lead to identification of the perpetrator.[85] Essentially, when a DNA sample from a crime scene does not match any samples available in CODIS, these private databases provide an alternative option. Since law enforcement began utilizing GEDmatch for investigation purposes, 59 cold cases have been solved and 11 John Doe identifications have been made.[86] Curtis Rogers, the owner of GEDmatch, stated that GEDmatch has never identified the criminal specifically, and instead provides a list of relatives of the suspect (or persons of interest).[87] Using traditional forensic methods, law enforcement is then able to narrow that list to a region, family, or individual by building a family tree.[88]

---

82 Katelyn Smith, *Genealogy Database Privacy Change Creates Challenges for Investigators*, WGAL8 (Sept. 6, 2019), https://www.wgal.com/article/genealogy-database-privacy-change-creates-challenges-for-investigators/28945357.

83 *Id.*

84 Sarah Zhang, *The Coming Wave of Murders Solved by Genealogy*, THE ATLANTIC (May 19, 2018), https://www.theatlantic.com/science/archive/2018/05/the-coming-wave-of-murders-solved-by-genealogy/560750/.

85 *Id.*

86 Vicki Gonzalez, *How DNA Ingenuity Led to Wave of Cold Case Arrests*, KCRA3 (Apr. 25, 2019), https://www.kcra.com/article/dna-cold-case-arrests-golden-state-killer-norcal-rapist/27245135.

87 *Id.*

88 *Id.*

The manner in which the Golden State Killer, among many others,[89] have been found is becoming increasingly controversial. Aside from undermining individual privacy rights, other dangerous consequences lurk in the practice of matching DNA markers against large databases. A prime example of such dangers is revealed in the case of Michael Usry, Jr.[90] Usry was targeted by the Idaho Falls police as a suspect in the 1996 murder of Angie Dodge.[91] A partial match between a semen sample found at the scene and the genetic profile of Usry's father, Michael Usry Sr., led the police to Usry.[92] The elder Usry had submitted his DNA for testing to a nonprofit DTC genealogy company called Sorenson Molecular Genealogy Foundation (which has since been acquired by Ancestry.com).[93] After extensive research into the DNA of the Usry family, Michael Jr. was identified.[94] The detectives persuaded a judge to sign a warrant ordering Michael Jr. to provide DNA for comparison.[95] Michael Jr. denied any connection to the rape or murder of Dodge, but complied with the court order.[96] While waiting for the test results, Michael Jr. lived in a state of anger, shock, and fear of not knowing whether he would be serving the rest of his life in prison due to a DNA misidentification.[97] Ultimately, Michael Jr. was determined innocent, but the process was nonetheless an imposition on his life.

As the capabilities of these services continue to develop, it is likely that the public will increasingly continue to use them, hence the compelling need for broader genetic privacy protections. The advancement of this technology makes identification of individuals easier, but also potentially invites abuse of individuals' fundamental rights, especially for victims of misidentification such as Michael Usry Jr.

---

89 *See* Justin Jouvenal, *The Unlikely Crime-fighter Cracking Decades-old Murders? A Genealogist*, WASHINGTON POST (July 16, 2018), https://www.washingtonpost.com/local/public-safety/in-decades-old-crimes-considered-all-but-unsolvable-genetic-genealogy-brings-flurry-of-arrests/2018/07/16/241f0e6a-68f6-11e8-bf8c-f9ed2e672adf_story.html (William Earl Talbott II caught using GEDmatch); Jeff Hawkes & Tom Knapp, *Raymond 'DJ Freez' Rowe Arrested for 1992 Killing of Schoolteacher Christy Mirack*, LANCASTERONLINE, (June 25, 2018), https://lancasteronline.com/news/local/raymond-dj-freez-rowe-arrested-for-killing-of-schoolteacher-christy/article_f05a2ee4-78b2-11e8-ad10-4382ef42f96d.html (Raymond 'DJ Freez' Rowe is arrested after being linked to a 1992 rape and murder through the use of GEDmatch).

90 Anne Marie Green, *How Safe is Your DNA?*, CBS NEWS, (June 16, 2018), https://www.cbsnews.com/news/how-safe-is-your-dna-familal-search-privacy-rights/.

91 *Id.*

92 Jim Mustian, *New Orleans Filmmaker Cleared in Cold-case Murder; False Positive Highlights Limitations of Familial DNA Searching*, THE NEW ORLEANS ADVOCATE (Mar. 12, 2015), https://www.theadvocate.com/new_orleans/news/article_1b3a3f96-d574-59e0-9c6a-c3c7c0d2f166.html.

93 *Id.*

94 *Id.*

95 *Id.*

96 *Id.*

97 Green, *supra* note 90.

C. Supreme Court Precedent: Genetic Privacy Under the Fourth Amendment

The following discussion highlights the fluidity of judicially imposed privacy protections under the Fourth Amendment in order to show why legislation is the proper method of enforcement. Because a general right to privacy does not expressly exist under federal constitutional law, the Supreme Court found privacy rights in the "penumbras" and "emanations" of other constitutional protections such as the Third, Fourth, and Fifth Amendments.[98]

During the ratification of the Constitution, Patrick Henry warned that the Federal Constitution would expose citizens to searches and seizures "in the most arbitrary manner, without any evidence or reason."[99] Thus, the Fourth Amendment to the Constitution was drafted and ratified to guarantee the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[100]

> A close examination of history indicates two principal forces helped to create the desire for protection against governmental searches and seizures to be included in the Constitution. The first of these was the history of abuses of personal privacy in Great Britain and the second was a similar history in the American colonies.[101]

The purpose of the Fourth Amendment was to prevent general and open-ended searches by law enforcement officers of any person, for any reason, at any time.[102]

As interpreted by the Supreme Court, warrants, probable cause, exigency, and good faith are demanded of law enforcement by the Fourth Amendment.[103] In order to search, the Amendment's Warrant Clause requires "probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[104]

---

98 Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

99 3 Debates on the Federal Constitution 588 (J. Elliot 2d ed. 1854).

100 U.S. CONST. amend. IV.

101 THOMAS N. MCINNIS, THE EVOLUTION OF THE FOURTH AMENDMENT 15, LEXINGTON BOOKS (2009).

102 *E.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 453 (1971) (determining that a government enforcement agent does not have the authority to issue a warrant. A warrant must be issued by a neutral and detached magistrate. The plain-view doctrine does not allow police to conduct warrantless searches of automobiles who expect in advance to find evidence).

103 Whren v. United States, 517 U.S. 806, 812-13 (1996) (holding that objective reasonableness is the test, subjective intent does not make an otherwise lawful conduct illegal or unconstitutional); Payton v. New York, 445 U.S. 573, 585-86 (1980) (holding that absent some other exigent circumstance, an officer cannot routinely enter a home without a warrant to make an arrest).

104 U.S. CONST. amend. IV.

Without a warrant or one of the narrow, judicially-created exceptions to the warrant requirement, the search and seizure may be characterized as unreasonable and thus, violative of the Fourth Amendment.[105] All of these demands, however, are measured by one criteria: reasonableness.[106]

In an attempt to uphold the core requirements demanded by the Constitution and additionally keep up with society's moral and political climate, the Supreme Court is constantly changing and limiting the Fourth Amendment. A history of these fluctuations is necessary in order to highlight the inadequacy of the Amendment in the context of genetic privacy rights.

1. Shifting the Focus from Property to Privacy

Initially, Fourth Amendment protections were grounded in common law property concepts and limited to the physical penetration of the four enumerated items—persons, houses, papers, and effects.[107] *Warden v. Maryland* and *Katz v. United States* shifted the focus of Fourth Amendment protections. The Court in *Warden* held that the nature of the property seized is irrelevant and discarded the premise that property interests control search and seizure.[108] In deciding *Katz*, the Court stated that the Fourth Amendment protected people, not places, making privacy the focal point of Fourth Amendment protections.[109] To that effect, Justice Harlan, in a concurring opinion, established the reasonable expectation of privacy standard.[110] This standard provides: to have a protected privacy interest, an individual must exhibit an actual, subjective expectation of privacy that society is prepared to recognize as reasonable.[111]

Cases following *Katz* returned property to the central role but often complicated it by subsuming property under the reasonable expectation of privacy formula, making property rights a way in which an individual has a

---

105 There are many exceptions to the warrant requirement. *See, e.g.*, Kentucky v. King, 563 U.S. 452 (2011) (exigent circumstances); Arizona v. Gant, 556 U.S. 332 (2009) (a search incident to lawful arrest); Illinois v. Rodriguez, 497 U.S. 177 (1990) (consent); Texas v. Brown, 460 U.S. 730 (1983) (plain view); United States v. Santana, 427 U.S. 38 (1976) (destruction of evidence during hot pursuit of fleeing felon); Terry v. Ohio, 392 U.S. 1 (1968) (stop and frisk); Carroll v. United States, 267 U.S. 132 (1925) (automobile exception).

106 Vernonia School District 47J v. Acton, 515 U.S. 646, 652 (1995) ("[T]he ultimate measure of the constitutionality of a governmental search is 'reasonableness.'"); Illinois v. McArthur, 531 U.S. 326, 330 (2001) (emphasizing that reasonableness is a central requirement).

107 Olmstead v. United States, 277 U.S. 438, 464 (1928) (holding electronic eavesdrop without a physical trespass is not a search under Fourth Amendment principles because the "[A]mendment itself shows that the search is to be of material things").

108 Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294, 304 (1967).

109 Katz v. United States, 389 U.S. 347, 351 (1967).

110 *Id*. at 360-61 (Harlan, J., concurring).

111 *Id.* at 361.

reasonable expectation of privacy.[112] Still, while it may seem that the *Katz* approach extends Fourth Amendment protections to all private areas of a person's life, the four enumerated protected items remain central to the scope of what is protected under the Amendment.[113]

The Supreme Court created a hierarchy of privacy interests, affording the greatest protection to expectations of privacy "society is 'prepared to recognize as legitimate,'"[114] less protection to a diminished expectation of privacy (thus allowing a search to be more easily justified),[115] and no protections for subjective expectations not recognized by society as legitimate.[116] It was not until 2012 in *United States v. Jones*, forty-five years after *Katz*, that Justice Scalia made clear that the *Katz* expectation of privacy standard did not replace the common-law trespassory test but supplemented it—expanding Fourth Amendment protection.[117]

2. Diminishing Your Privacy Rights

The second category in the hierarchy of privacy interests—diminished expectation of privacy—involves an interest that would otherwise be protected, but due to surrounding circumstances the interest is lower, and thus the search is more easily justified. For instance, the Supreme Court has applied a broad assumption of risk principle to the sharing, or voluntary exposure, of items, information, or space to a third party.[118] This principle follows the logic that an individual has no protected interest in voluntarily disclosed information because once disclosed, he cannot have a subjective expectation of privacy in it.[119]

---

112 *See generally* Bond v. United States, 529 U.S. 334 (2000) (holding luggage taken on a bus is an "effect" and that Bond possessed a privacy interest in his luggage).

113 *See generally* California v. Greenwood, 486 U.S. 35 (1988) (holding warrantless search of trash left outside the curb does not violate the Fourth Amendment); United States v. Miller, 425 U.S. 435 (1976) (holding bank customers have no reasonable expectation of privacy in their bank records); Couch v. United States, 409 U.S. 322 (1973) (holding once records are provided to an accountant the individual has no legitimate expectation of privacy in the information contained in the tax records).

114 New Jersey v. T.L.O., 469 U.S. 325, 338 (1985) (quoting Hudson v. Palmer, 468 U.S. 517, 526 (1984)).

115 *E.g.*, Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 624-25 (1989) (upholding regulations that mandated suspicionless breath, blood, and urine testing for railway employees involved in train accidents and for those who violated certain safety rules because railway employees had a diminished expectation of privacy by reason of their participation in an industry that was regulated to ensure safety).

116 *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 148-49 (1978) (holding passenger in automobile cannot challenge legality of a vehicle's search because they do not have a legitimate expectation of privacy in passenger compartment of the vehicle).

117 United States v. Jones, 565 U.S. 400, 409 (2012).

118 *See generally* United States v. Miller, 425 U.S. 435 (1976); California v. Greenwood, 486 U.S. 35 (1988).

119 *Miller*, 425 U.S. at 442-43.

One major Supreme Court decision, applying the third-party doctrine, held that there is no legitimate expectation of privacy in bank records released to a bank.[120] The Court determined that once the documents are given to the bank they are no longer an individual's private papers to which he may assert possession or ownership, despite how personal or pervasive the information in the documents may be.[121] Accordingly, law enforcement did not need to meet the high standards required to obtain a warrant in order to acquire the bank records; instead, a subpoena was sufficient.[122]

In another decision, the Court held that law enforcement's installation of a pen register to record phone numbers an individual dials does not constitute a search within the meaning of the Fourth Amendment.[123] The reason being was that a law enforcement official could not determine, from the use of a pen register, the contents of a phone call, the identities of the callers, nor whether the call was even completed.[124] Since the pen register had such limited capabilities, the Court analyzed whether the installation could constitute a search on the grounds that the Petitioner had a legitimate expectation of privacy in the phone numbers he dialed. This claim was rejected because of the unlikelihood that people had any subjective expectation of privacy in the phone numbers they dialed because phone numbers are conveyed to the telephone company for a variety of reasons, every day.[125]

Although bank records and pen registers contain information personal to the individual, the Court's rationale in concluding that neither is a protected privacy interest was rooted in the third-party doctrine. Thus, once a check or deposit slip is handed to a bank teller or a phone number is dialed, the disclosing individual can no longer expect that the information will remain private.

Privacy expectations are also diminished in certain institutions due to the government's greater interest in safety. Such institutions include jails, prisons, and schools. Where law enforcement is generally prohibited from conducting random searches of an individual's person, prisoners may be searched absent any suspicion[126] and students may be searched if there is reasonable, individualized suspicion the student has broken the law or a school rule.[127]

---

120 *Id.* at 442.

121 *Id.* at 443.

122 *Id.* at 446.

123 Smith v. Maryland, 442 U.S. 735, 743 (1979).

124 *Id.*

125 *Id.* (specifying that telephone companies send monthly statements to consumers, and thus, a reasonable consumer is on notice that the phone company is keeping such records for business purposes, such as charging extra for long distance phone calls).

126 Florence v. Bd. of Chosen Freeholders of the Cty. of Burlington, 566 U.S. 318, 330 (2012).

127 New Jersey v. T.L.O., 469 U.S. 325, 341-42 (1985).

Previous Fourth Amendment challenges to DNA data banking statutes have survived on the basis that the societal value outweighed the diminished privacy interests of convicted felons.[128] However, now that data banks have expanded to private ownership and consist of DNA belonging to non-convicts, individual privacy interest implications become quite different.

There are limited circumstances in which "the Government's interests are sufficiently compelling to justify an intrusion on privacy entailed by conducting [a] search[] without any measure of individualized suspicion."[129] Justice Scalia stated in a dissenting opinion, "[S]olving unsolved crimes is a noble objective, but it occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless law-enforcement searches."[130] When the Court held that collecting DNA from arrestees and storing the information in a database was permitted, it justified its decision by promising that it would not affect just any individual, only those arrested for "dangerous offenses."[131] That holding, therefore, cannot justify law enforcement's unfettered access to DNA evidence of those not arrested, convicted, or even suspected of a crime.

Further, the Court analogized the taking of DNA from an arrestee to other administrative identification methods such as matching a face to a wanted poster, tattoos to a gang affiliation, or fingerprints of the arrestee to those found at the crime scene.[132] Ultimately the Court decided that the government's interest in identifying and overseeing offenders and arrestees outweighed the appellants' privacy interests.[133]

The analogy the Court makes to fingerprinting is flawed for multiple reasons. Namely, in this case the Court was not concerned with the shared nature of DNA; at issue was only one specific arrested individual. Now that familial searching and utilization of private data banks is at issue, the Court's analogy misses a core issue: mutuality. Fingerprints are individualistic, meaning no two people have the same fingerprint.[134] Further, the Court focuses on similarity of the technique to obtain the data, while overlooking DNA's potential for revealing much more personal information than fingerprints ever could.[135] Collection of DNA crosses Fourth Amendment

---

128 Maryland v. King, 569 U.S. 435, 456 (2013).

129 Johnson v. Quander, 440 F. 3d 489, 494 (D.C. Cir. 2006) (citing Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 668 (1989)).

130 *King*, 569 U.S. at 481.

131 *Id.* at 463.

132 *Id.* at 451.

133 *Id.*

134 THOMAS P. MAURIELLO, 1 CRIMINAL INVESTIGATION HANDBOOK ¶ 14.05 (2019) ("[F]ingerprints are positive evidence that identifies an individual to the exclusion of all other human beings. It is estimated that the likelihood of two people having the same fingerprints is as high as 1 out of 10").

135 *King*, 569 U.S. at 451. The Court warned that the DNA evidence is not to be tested or analyzed for purposes other than administrative identification, but the Court has also said that only those arrested for dangerous offenses would be affected and that was easily changed.

boundaries when it is used for purposes beyond identifying offenders and arrestees, such as investigation of other crimes. These values, however, have not yet been explicitly recognized as legitimate by the courts because the justification of catching criminals is often greater. Consequently, it is difficult to mold the current Fourth Amendment landscape to fit the need for genetic privacy rights.

3. The Impact of Advancing Technology on Fourth Amendment Jurisprudence

Under our current understanding of a search, it may be easy to tell whether a police officer has come into a home, rummaged through a purse, or put his hands into a pocket; but, the progression of technology has made a search possible without any such detectable physical intrusion.

The home is considered "first among all equals" for Fourth Amendment purposes.[136] At the very core of Fourth Amendment protections is "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusions."[137] Thus, law enforcement's warrantless entry into private dwellings and areas immediately surrounding, is consistently determined violative of Fourth Amendment principles under both the *Katz* analysis and the *Jones* common law trespass analysis.[138]

This time-honored ideology is perfectly illustrated in *Kyllo v. United States*, in which the Court considered the effects of technology, and enhanced abilities to examine a private space without a physical intrusion, on fundamental rights.[139] There, the Court struck down law enforcement's use of a thermal imager to detect heat radiating from the side of defendant's home.[140] This was determined a search because "[t]o withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."[141] The new rule established

---

136 Florida v. Jardines, 569 U.S. 1, 6 (2013) (holding that police, like all other individuals, have license to walk up to the front door of a dwelling, and that it is an unconstitutional trespass of this license to bring a drug sniffing dog to investigate the contents of the home from the outside of the dwelling).

137 *Id.*

138 *See e.g., id.;* Kyllo v. United States, 533 U.S. 27 (2001); Arizona v. Hicks, 480 U.S. 321 (1987) (holding that authority to search a dwelling for one purpose does not automatically give law enforcement free reign and deviating from that one purpose constitutes a separate search for Fourth Amendment purposes); Payton v. New York, 445 U.S. 573 (1980) (holding warrantless searches and seizures within a home are presumptively unreasonable); *cf.* California v. Ciraolo, 476 U.S. 207 (1986) (holding that law enforcement's aerial search of a garden behind the home is not a search under the Fourth Amendment); and United States v. Dunn, 480 U.S. 294 (1987) (holding a barn behind the home falls outside the area protected under the home's umbrella of Fourth Amendment protection).

139 *Kyllo*, 533 U.S. 27, 29 (2001).

140 *Id.* at 40.

141 *Id.* at 34.

in *Kyllo* was written broadly to account for "more sophisticated systems that are already in use or in development," and not just the thermal imager at issue in that case.[142]

Justice Stevens, along with three other Justices, disagreed with the majority arguing that such a rule is "unnecessary, unwise, and inconsistent with the Fourth Amendment."[143] The dissenting Justices felt that it would be wiser to allow legislators an opportunity to handle these evolving matters rather than fashioning such an all-encompassing rule that may restrict their efforts.[144]

The Court was again presented with an issue created by the misuse of technology in *United States v. Jones*, a case involving the placement of a GPS tracking device by law enforcement under a suspect's vehicle.[145] Instead of applying the *Katz* privacy test (which likely would have led to the same result), the Court used the common law trespass test to conclude that law enforcement had violated the Fourth Amendment because the officers' act of placing the tracker under the car was a physical intrusion of a protected interest.[146]

In a concurring opinion, Justice Alito suggested that it would be more appropriate to decide this case using the *Katz* approach because the trespass test, as originally understood, could not have accounted for situations involving today's technology.[147] Justice Alito forewarned that, as applied to advancing technology and individual privacy, the *Katz* "reasonable expectation of privacy" test is problematic.[148] The reason being that "[n]ew technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile."[149] Thus, as technology advances, society's set of privacy expectations may change. Accordingly, privacy concerns should be addressed by the legislative branch because it is in the best position "to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[150]

Only two years later, the Court determined that a modern cell phone implicated privacy concerns far greater than any other physical record.[151] The quantity and quality of information discoverable in a single cell phone

---

142 *Id.* at 36.
143 *Id.* at 41 (Stevens, J. dissenting).
144 *Id.* at 51.
145 United States v. Jones, 565 U.S. 400, 402 (2012).
146 *Id.* at 410-14.
147 *Id.* at 418-19.
148 *Id.* at 427-28.
149 *Id.* at 427.
150 *Id.* at 429-30.
151 Riley v. California, 573 U.S. 373, 395 (2014).

obligated the Court to limit law enforcement's ability to search.[152] Generally, police officers have authority to search an arrestee's person by virtue of the lawful arrest.[153] However, if a cell phone is found during the search, absent any exigent circumstances, a warrant must be obtained prior to searching the contents of the phone.[154] Once again, Justice Alito concurred, insisting that the federal courts should not be using the Fourth Amendment as a tool to construct privacy protections.[155] Legislators, who are elected by the people, are better positioned to address such privacy concerns and "it would be very unfortunate if privacy protections in the 21st century were left primarily to the federal courts."[156]

Similarly, in *Carpenter* the Court held that an individual has a legitimate expectation of privacy in cell-site records and that accessing those records without a warrant constituted a search.[157] The Court recognized the following:

> Although no single rubric definitively resolves which expectations of privacy are entitled to protection, the analysis is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure "the privacies of life" against "arbitrary power." Second, and relatedly, that a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance."[158]

Cell phone location information is "detailed, encyclopedic, and effortlessly compiled,"[159] and provides police officers "an intimate window into a person's life."[160] The retrospective quality of the data to which police would have access to was also taken into consideration.[161] Since location information is continually logged for all of the 400 million devices in the United States, the tracking capacity runs against virtually everyone.[162] Phone companies keep this information for five years, thus, whoever the suspect turns out to be, the police will have information detailing his or her location

---

152 *Id.* at 393.

153 THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 427 (2d ed. 2014).

154 *Riley*, 573 U.S. at 386.

155 *Id.* at 404.

156 *Id.* at 407-08.

157 Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018). Cell-site location information is the time-stamped record that is generated each time a phone connects to a cell-site. Smartphones tap into wireless networks looking for the best signal which comes from the nearest cell-site.

158 *Id.* at 2214.

159 *Id.* at 2209.

160 *Id.* at 2217.

161 *Id.* at 2218.

162 *Id.*

on every day for the previous five years.[163] Despite existing precedent concerning the third-party doctrine, the Court determined, just as it did in *Kyllo*, the data cannot be retrieved without a warrant "because any other conclusion would leave homeowners 'at the mercy of advancing technology,' and the government—absent a warrant—could not capitalize on such new sense-enhancing technology."[164]

In this narrow opinion, the Court refused to apply established principles (search incident to arrest and third-party doctrine) to cell-site location information because of the extremely personal nature of the information contained in a cell phone. While analogous arguments may be made regarding genetic privacy, the Court specifically stated that the *Carpenter* decision is a narrow one that does not extend to matters not before the Court, disturb *Smith* or *Miller*, question other surveillance techniques, address other business records, or consider other collection techniques.[165] Even so, Justice Alito dissented to express his concern on future application of the *Carpenter* decision, again proposing legislation as the preferable method of addressing individual privacy rights. Alito discourages the development of new Fourth Amendment caselaw on this subject because of "the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope."[166]

D. Existing Statutory Law on Privacy

1. General Right to Privacy

In addition to judicially imposed privacy protections, privacy has long been recognized as essential to human and social well-being by state and federal legislators. Civil and criminal penalties have been implemented in an attempt to protect against invasions of privacy—specifically informational, medical, and genetic privacy.[167] The Federal Trade Commission Act (FTCA) broadly authorizes the United States Federal Trade Commission (FTC) to enforce federal privacy protection regulation by way of enforcement action against unfair or deceptive practices, including failure to comply with a company's own published privacy promises.[168] There is no general federal legislation impacting data protection and privacy, but rather sector-specific legislation that focuses on specific data.[169] For example, the

---

163 *Id.*

164 *Id.* at 2214.

165 *Id.*

166 *Id.* at 2261 (Alito, J., dissenting).

167 *See* STEVEN CHABINSKY & F. PAUL PITTMAN, THE ICLG TO: DATA PROTECTION LAWS AND REGULATIONS 18.1 (2019).

168 *Id.* at 1.1.

169 *Id.* at 1.2.

Gramm-Leach-Bliley Act (GBLA) protects personal information held by companies in the financial service industry;[170] the Fair and Accurate Credit Transactions Act (FACTA) requires that certain financial institutions hide credit card numbers on printed receipts and destroy certain personal information, regulates uses of personal information from affiliated companies for marketing purposes, and imposes obligations on financial institutions to help detect and respond to identity theft;[171] and the Family Educational Rights and Privacy Act (FERPA) prohibits the disclosure of student records or other personal information without the student's or parent's consent.[172]

The United States does not have a specific agency in charge of regulating data protection and privacy, but the FTC's authority is broad and generally leads on federal privacy issues. Additionally, the Department of Health and Human Services, the Federal Communications Commission, the Securities and Exchange Commission, the Consumer Financial Protection Bureau, and the Department of Commerce have passed sectoral laws to aid data protection.[173]

Federal law may pre-empt state law if both laws cover the same topic; however, by way of the Ninth and Tenth Amendments, individual states have the power to expand protections of rights not enumerated in the United States Constitution,[174] which they often do.

Constitutions in eleven states include explicit right to privacy provisions.[175] For example, Alaska's constitution states "the right of the people to privacy is recognized and shall not be infringed,"[176] and Montana's constitution recognizes "the right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."[177]

Further, state legislators have passed laws covering a variety of privacy concerns including social media privacy,[178] consumer data,[179] and digital

---

170 15 U.S.C. § 6802(a) (2010).

171 15 U.S.C. § 1681 (1970).

172 20 U.S.C. § 1232g (2013).

173 CHABINSKY & PITTMAN, *supra* note 167, at 1.4.

174 U.S. CONST. amends. IX, X.

175 These states include Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, New Hampshire, South Carolina, and Washington. NAT'L CONF. OF ST. LEGISLATURES, PRIVACY PROTECTIONS IN ST. CONST. (Nov. 7, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx.

176 ALASKA CONST. art. I § 22.

177 MONT. CONST. art. II § 10.

178 NAT'L CONF. OF ST. LEGISLATURES, ST. SOC. MEDIA PRIVACY LAWS (May 22, 2019), http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx.

179 NAT'L CONF. OF ST. LEGISLATURES, 2019 CONSUMER DATA PRIVACY LEGIS. (Jan. 1, 2020), http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

privacy and cyber security.[180] Every state has adopted some form of data breach notification legislation, varying only by what types of information is subject to the law.[181] California enacted the California Consumer Privacy Act (CCPA), which gives California residents the right to request access to and deletion of personal information, and the right to opt out of data sharing with third parties.[182] The new law, which went into effect on January 1, 2020, only applies to certain businesses and introduces new obligations to disclose information—such as sources from which personal information is collected, the business purpose for collecting personal information, and the categories of third parties with which personal information is shared.[183]

On a more international scale, the General Data Protection Regulation (GDPR), which took effect May 25, 2018, is a European Union (EU) privacy law regulating how certain organizations treat or use the personal data of people located in the EU.[184] Under this regulation, EU citizens have the right to ask for details about how their personal data is used as well as request certain things be done with their data.[185] Among other things, EU citizens will have the right to prohibit companies from sharing their personal data and may even demand their data be destroyed.[186] Ideally, the United States would follow in the EU's footsteps and enact broad legislation similar to the GDPR to protect individuals and their families who submit their personal information to a third party, but that is beyond the scope of this Note.

2. Genetic Privacy

Rather than implementing broad legislation to protect genetic information, the way the United States protects genetic data depends on where the data is and what it is being used for. The primary laws governing genomic medicine and policy are the Americans with Disabilities Act of 1990 (ADA),[187] the Clinical Laboratories Improvement Amendments of 1988 (CLIA),[188] the Genetic Information Nondiscrimination Act of 2008

---

180 NAT'L CONF. OF ST. LEGISLATURES, PRIVACY AND SECURITY, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-and-security.aspx (last visited Nov. 8, 2019).

181 NAT'L CONF. OF ST. LEGISLATURES, SECURITY BREACH NOTIFICATION LAWS (Sept. 29, 2018), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

182 CHABINSKY & PITTMAN, *supra* note 167, at 1.2.

183 CHABINSKY & PITTMAN, *supra* note 167, at 1.4.

184 Commission Regulation 2016/679 of Apr. 27, 2016 O.J. (L 119) 1.

185 *Id.*

186 *Id.*

187 42 U.S.C. ch. 126 § 12101 (1990).

188 42 U.S.C. § 263(a).

(GINA),[189] the Health Information Technology for Economic and Clinical Health Act, 2009 (HITECH),[190] the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[191] and the Patient Protection and Affordable Care Act, 2010 (ACA).[192] This system of independent sporadic coverage is flawed because it does not account for the complexity of DNA and its potential for uses beyond its original one.

For example, the 21st Century Cures Act ensures confidentiality of genetic information for any federal research subjects, including from law enforcement or any other government agency.[193] If the information were inadvertently disclosed or illegally obtained by law enforcement, it would be inadmissible in court.[194] If the individual provides the information to a primary care physician, it becomes "personal health data" governed by HIPAA.[195] Under HIPAA, the genetic information cannot be disclosed to schools or employers, but law enforcement is entitled to access it for investigation purposes and it may be admitted for civil or criminal trial.[196] Because the genetic information is now part of your health records, your insurance company has access to it, but because of GINA, the insurance company is prevented from denying coverage or increasing premiums on the basis of those genetic tests.[197] However, not all health insurance companies fall within GINA's jurisdiction and it does not apply to life insurance, disability insurance, or long-term care insurance.[198] Further, the genetic testing of parents are likely to reveal information regarding a child's genome. Despite the passage of GINA, current laws do not protect against all forms of discrimination and thus a child with a potential deleterious generic alteration may still be treated unfairly in schools, by health care providers, and possibly by peers.[199] Further, none of the foregoing laws or regulations apply to DTC genetic testing or account for privacy implications.

Two federal agencies have the authority to regulate genetic testing: the Food and Drug Administration (FDA) and the Centers for Medicare and

---

189 Genetic Information Nondiscrimination Act, Pub. L. 110 § 233, 122 Stat. 881 (May 21, 2008) [hereinafter GINA].

190 Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5 § 3001, 123 Stat. 115 (Feb. 17, 2009) [hereinafter HITECH].

191 The Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, § 264, 110 Stat. 1936 (1996) [hereinafter HIPAA].

192 Patient Protection and Affordable Care Act of 2010, Pub. L. No. 111-148, 124 Stat 119, amended by Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029 (codified as amended in scattered statutes of 42 U.S.C.).

193 Pub. L. No. 114 § 255, 130 Stat. 1033 (2016).

194 *Id.*

195 HIPAA, Pub. L No. 104-191, § 264, 110 Stat. 1936 (1996).

196 *Id.*

197 GINA, Pub. L. 110 § 233, 122 Stat. 881 (May 21, 2008).

198 *Id.*

199 Janet Dolgin & Lois Shepherd, Bioethics and the Law, 219 (4th ed. 2019).

Medicaid Services (CMS).[200] CMS regulates clinical laboratories conducting genetic testing to ensure that the procedures used meet quality standards and that the technicians performing the tests are qualified.[201] The FDA considers genetic testing as a medical device, and thus, has authority to regulate any such diagnostic tools.[202] However, whether the FDA regulates a genetic test depends on how it comes to the market. Commercial test kits (which are packaged together and sold to laboratories) must be approved by the FDA before the product may be introduced to the market.[203]

On the other hand, laboratory-developed tests (LDT), those which are developed and performed by one lab, are used without FDA assessment of validity.[204] With the growth of DTC genetic testing, the FDA is modifying its approach due to concerns that unregulated tests pose a public health threat.[205] On the other hand, the Department of Justice (DOJ) has authority to regulate law enforcement practices and procedures. The DOJ's Interim Policy on forensic genetic genealogy went into effect on November 1, 2019.[206] The Policy states that the DOJ "must use [forensic genetic genealogical DNA analysis] in a manner consistent with the requirements and protections of the Constitution and other legal authorities."[207] The Policy only applies to federal agencies and state and local agencies that receive grant award funding from the federal government. The Policy further limits the use of this type of DNA analysis to solving homicide and sexual offense cases and the identification of human remains. A prosecutor may authorize the investigation for violent crimes other than homicide or sexual offenses "when the circumstances surrounding the criminal act(s) present a substantial and ongoing threat to public safety or national security."[208] Before law enforcement may use private databases, all other investigation methods must be exhausted, and the forensic profile must have been uploaded to CODIS and failed to produce any DNA matches. Additionally, the Policy forbids the use of biological samples for all purposes beyond investigation of the crime, including testing for psychological traits or predispositions to disease. The DOJ announced that the final policy is scheduled to be issued in 2020.[209]

---

200 NAT'L HUM. GENOME RES. INST., REG. OF GENETIC TESTS, NIH (Jan. 17, 2018), https://www.genome.gov/about-genomics/policy-issues/Regulation-of-Genetic-Tests.

201 *Id.*

202 *Id.*

203 *Id.*

204 *Id.*

205 *Id.*

206 U.S. Department of Justice, Interim Policy, Forensic Genetic Genealogical DNA Analysis and Searching 1 (2019).

207 *Id.*

208 *Id.*

209 Office of Public Affairs, *Department of Justice Announces Interim Policy on Emerging Method to Generate Leads for Unsolved Violent Crimes*, UNITED STATES DEPARTMENT OF JUSTICE (Sept.

The DNA Identification Act of 1994 ensures DNA data stored in CODIS is confidential.[210] Further, so long as genetic information is stripped of any identifiable information, it may be accessed by criminal justice agencies for population statistics, identification research, protocol development, or quality control.[211] However, scientists have indicated that with enough data, re-identifying genetic information is very much possible.[212]

It is evident that the authority to regulate exists, thus further steps need to be taken to account for genetic privacy, along with validity and quality assurance. Additionally, evidence that Congress is prepared to recognize an individual's protected privacy interest in the shared DNA of a family member is found in the definitions section of GINA. Congress defined "genetic information" to include "information about [an] individual's genetic tests, the genetic tests of family members of such individual, and the manifestation of a disease or disorder in family members of such individual."[213] Existing federal privacy regulations in the United States—whether legislative or judicial—are insufficient to adequately protect our shared privacy interests implicated by genetic information.

Currently only about half of the states have laws or regulations governing genomic privacy.[214] Some of these states provide for more protection, prohibiting the unauthorized acquisition and analysis of genetic information, while others only prohibit unauthorized disclosure of DNA information.[215] Whether genetic testing can be performed without the consent of the donor depends on many factors such as who is seeking to conduct the test, what the tests are for, how results will be used, and the state in which the testing takes place.[216]

While some states provide for more protection, all states are required to follow HIPAA, mandating genetic information be de-identified before it can be shared.

In 2018, Louisiana became the first state to enact legislation covering DTC testing kits.[217] The law demands any company selling such kits provide consumers with an easy to read notice informing individuals on how DNA is used, whether it can be used for other purposes, whether it will be shared

---

24, 2019), https://www.justice.gov/opa/pr/department-justice-announces-interim-policy-emerging-method-generate-leads-unsolved-violent.

210 34 U.S.C. § 12592 (transferred from 42 U.S.C. § 14132).

211 *Id.*

212 Mats G. Hansson et al., *The Risk of Re-Identification Versus the Need to Identify Individuals in Rare Disease Research*, 24 EUR. J. OF HUM. GENETICS 1553, 1555 (2016).

213 110 Pub. L. 233, 122 Stat. 881.

214 *Privacy in Genomics*, NAT'L HUM. GENOME RES. INST. (Jan. 17 2020), https://www.genome.gov/27561246/privacy-in-genomics/.

215 *Id.*

216 *Id.*

217 LA. REV. STAT. § 51:3151 (2018).

with third parties, whether the consumer has the ability to request the information be destroyed, and whether the consumer relinquishes ownership of the information once it is disclosed.[218] This is a positive step forward in that it acknowledges and highlights the individual's right to be informed—a major aspect of privacy rights.

Due to a lack of uniformity between the federal and state governments in addressing the importance of genetic privacy, even the existing safeguards are unworkable. For example, Maryland and Washington D.C. expressly prohibit familial searching by law enforcement, but there is nothing stopping law enforcement in other jurisdictions from conducting familial searches based on samples from Maryland arrestees or convicts and thus implicating their relatives.

The threat to privacy faced by American citizens today is not a consequence of advancing technology that we must simply become accustomed to. The greatest threat stems from powerful law enforcement agencies that exploit personal data and justify their practices as essential investigative techniques. Because the protection of genetic privacy affects every American, Congress is in the best position to address these concerns and provide the necessary protections.

E. Government Abuses of Genetic Information

A government database encompassing the genetic information of all its citizens would be detrimental to every individual as well as to society as a whole. Most of the laws in place today were enacted in response to various infringements on individual rights. Although we have not yet experienced the repercussion that may stem from allowing the government access to private DNA databanks, a statute addressing potential abuse is not premature.

Privacy concerns about genetic information resemble privacy concerns about other forms of medical information. A controversial aspect of this is highlighted in newborn screening programs—but more specifically in the retention of DNA information obtained from the screening programs. In one case, *Beleno v. Lakey*, a group of parents claimed that the Texas Department of State Health Service, among others, seized blood samples taken from babies at the time of birth.[219] The blood samples were stored indefinitely for undisclosed purposes, without the consent of parents. The parties ultimately settled, and pursuant to the settlement agreement, the Department was to destroy all blood specimens obtained as a part of the program.[220] During the pendency of the case, the state legislature amended the relevant statutory law

---

218 *Id.*

219 Beleno v. Lakey, Civil Action No. SA-09-CA-188-FB (USDC W.D. Tex. Sept. 17, 2009).

220 Higgins v. Tex. Dept. of Health Servs., 801 F. Supp. 2d 541, 545-46 (USDC W.D. Tex. 2011).

to allow for informed consent by the parents, including the right to limit the use of the genetic material.[221]

Another cause for concern with an all-encompassing genetic database may lead to Government encouraging or requiring testing for certain hereditary diseases—they would not have to encourage it, they could just do the test themselves if they had the databank. Workers' Compensation litigation could be severely altered if employers had access to such databases to negate causation. For instance, an employee who suffered a back injury at work may lose benefits if the employer could show that the employee has a gene linked to degenerative disc disease.

There are lessons to be learned from past, misguided programs established by the government. In the early 1970s, legislators were pressed to pass mandatory sickle hemoglobin screening laws requiring certain individuals to get tested for sickle-cell disease. Researchers found that

> These programs led to: (1) stigmatization of potentially two million African-Americas with sickle cell trait; (2) mandatory sickle hemoglobin screenings laws in twelve states (including the District of Columbia); some were quite subtle, others were not . . .; (3) increased insurance rates for persons with sickle cell trait [. . .]; (4) the firing of flight attendants with sickle cell trait; (5) rejection of persons with sickle cell trait from flight and other hazardous service in the Armed Forces; (6) the banning of persons with sickle cell trait from athletics [. . .]; and (7) sterilization of carriers of sickle hemoglobin.[222]

While it may seem unlikely for the government to initiate a program of mass genetic testing today, there are several instances in which the government has justified intrusions on the individual by placing public health over personal autonomy. Current vaccination laws provide one such example. State vaccination laws, with very few exemptions, include requirements for children in public and private schools and day cares, students at public colleges and universities, and healthcare workers to be vaccinated as a prerequisite for attending the facility.[223]

To a lesser extent, state policies encouraging prenatal care and carrier screening may cause prospective parents to feel compelled to avoid having children whose genetic health is less than that which is desired. Carrier screenings that detect positive results for certain diseases or defects can lead

---

221 *Id*. at 544-45.

222 James E. Bowman, The Plight of Poor African-Americans: Public Policy on Sickle Hemoglobin and AIDS, in African-American Perspectives on Biomedical Ethics (Harley E. Flack & Edmund D. Pellegrino, eds. 1992), at 173, 192.

223 Public Health Professionals Gateway, *Vaccination Laws*, CENTERS FOR DISEASE CONTROL AND PREVENTION (Feb. 28, 2018).

to abortions, stigmatization, and discrimination.[224] A study done in Australia concluded that only five percent of pregnancies in which the fetus was diagnosed with Down syndrome, following a prenatal carrier screening, resulted in a live birth.[225]

Government tampering with genetic information is as, if not more, prevalent today as it was in the past. Allowing an easy-access database with the genetic information of virtually every individual will have unimaginable consequences and needs to be regulated before any misuse occurs.

III. ANALYSIS

Anita Allen labelled the four categories of genetic privacy as (1) informational privacy (concerning access to personal information); (2) physical privacy (concerning access to personal space); (3) decisional privacy (concerning governmental interference with personal choices); and (4) proprietary privacy (concerning ownership of interest in human personality).[226]

Accounting for the complexity embedded in DNA requires a legal framework that will accommodate both individual and shared privacy interests as well as informational and decisional dimensions of privacy. Only Congress has the power to appropriately address such an issue because neither the privacy nor property approaches established by the Supreme Court are adequate to fully address the issue without expanding the protections of the Fourth Amendment even further. This is because a privacy approach is individualistic in nature and thus, alone, inadequate when analyzing overlapping, shared interests; and property concepts, as they stand, would limit Fourth Amendment application to the initial procurement of the physical DNA.

A. DNA's Appearance in Court

Most rulings in cases presented to the courts concerning DNA or tissue ownership have been against the patient.[227] Courts generally rule in favor of informed consent contracts and third-party doctrine principles over individual privacy rights or unauthorized subsequent usage.[228]

---

224 Dolgin, *supra* note 199, at 208-09.

225 Veronica R. Collins et al., *Is Down Syndrome a Disappearing Birth Defect?*, J. PEDIATR. 152(1) (2008), 20-24.

226 Anita L. Allen, *Genetic Privacy: Emerging Concepts and Values*, in GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 31, 33 (Mark A. Rothstein ed., 1997).

227 *Ownership of Genetic Information*, GENETICS GENERATION (2015), http://knowgenetics.org/ownership-of-genetic-information/ (last visited Feb. 16, 2019).

228 *Id.*

Furthermore, suing based on the unauthorized testing of voluntarily submitted DNA may present a challenge as well. The requirement that initial procurement of DNA must pass constitutional muster logically follows the long-standing principles established by the Supreme Court.[229] Whether the Fourth Amendment may be implicated after initial procurement has not been expressly ruled upon, but the Court in *Maryland v. King* suggested that the process of collection and testing the specimen are two separate events, each subject to constitutional protections.[230]

In deciding that the Fourth Amendment permits warrantless breath tests following a lawful arrest for drunk driving but not warrantless blood tests, the Court evaluated the impact of breath and blood tests on individual privacy interests.[231] A significant distinction found by the Court concerned the potential for preservation of blood for unauthorized, future testing.[232] The Court's recognition of the privacy concerns associated with subsequent unauthorized use of DNA, is further evidence demonstrating the need for legislation.

B. Issues Getting to Court

1. Who Can Sue

The Fourth Amendment protects only "the right of the people to be secure in *their* persons, houses, papers, and effects."[233] Even after the *Katz* decision broadened Fourth Amendment principles, the Supreme Court interpreted Fourth Amendment rights to be personal,[234] and expressly limited the expectation of privacy to only that which belongs to the individual.[235] Thus, to establish standing, one must show that a governmental search has invaded his or her legitimate expectation of privacy.[236] To have a legitimate expectation of privacy, there must be a reference to real or personal property or the privacy interest must be one that is understood and permitted by

---

229 Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 617-18 (1989) (noting that compulsory extraction of blood for DNA profiling, breathalyzer tests, and the collection and testing of urine have been deemed searches due to concerns about bodily integrity).

230 *See* Maryland v. King, 569 U.S. 435 (2013).

231 Birchfield v. North Dakota, 136 S. Ct. 2160, 2163 (2016).

232 *Id.* at 2178.

233 CONST. amend. IV.

234 Rakas v. Illinois, 439 U.S. 128, 140 (1978).

235 *See* Rawlings v. Kentucky, 448 U.S. 98 (1980).

236 THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 141 (2d ed. 2014).

society.[237] Homeowners,[238] boarders,[239] apartment tenants,[240] and others living in a dwelling[241] have standing to challenge a search of their home by virtue of having a legitimate expectation of privacy inside the home (stemming from their right to exclude).[242] The right to exclude is a basic, legally recognized aspect of home ownership.[243] However, in the current situation, defendants have exclusively been family members of individuals who submitted their DNA for testing to the DTC company, and thus have no meaningful control over any of the personal data. The defendant does not have a right to access the results, to prevent or demand destruction of the data, or to modify it in any way. All of these rights are held by the initial consumer, who waived many of his or her privacy rights when signing the terms and conditions policy.

What existing Fourth Amendment precedent fails to account for is the shared nature of DNA. As DNA is shared to such a large degree among relatives, it is appropriate to recognize that the submitted genetic information belongs to each individual member of the family. If we are to accept that idea, each relative would appropriately have standing to challenge an unreasonable search of their shared DNA, much as they would have standing to challenge an unconstitutional search of their shared residence. However, as Fourth Amendment principles stand, the only individual with standing to challenge the disclosure of DNA to a third party is the one who submitted it.

Privacy rights might also be implicated when law enforcement (or in this case, Paroban Nanolabs which was hired by law enforcement) submits genetic information found at a crime scene to a DTC genealogy testing company. This becomes an issue when there is DNA at the crime scene that, unbeknownst to the police, does not belong to the suspect but is then submitted for testing anyway. Additionally, the treatment of the genetic information after its submission remains a question. Does the DTC company retain the genetic information for their own use? Can the company sell the genetic information to researchers? Does the company return the data or destroy it? Whatever the subsequent treatment of the genetic information is, it is likely that a reviewing court would determine that the evidence left at the crime scene was abandoned, and consequently, its collection and subsequent testing was reasonable.

---

237 Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978).

238 Alderman v. United States, 394 U.S. 165 (1969).

239 McDonald v. United States, 335 U.S. 451, 454-56 (1948).

240 Chapman v. United States, 365 U.S. 610 (1961).

241 Bumper v. North Carolina, 391 U.S. 543 (1968) (deciding grandson could challenge unreasonable search of grandmother's home because he lived there).

242 Thomas W. Merill, *Property and the Right to Exclude*, 77 NEB. L. REV. 730, 730 (1998) ("The right to exclude is more than just 'one of the most essential constituents of property—it is the sine qua non.'").

243 *Id.*

2. Who Can Be Sued

As discussed above, to sue on Fourth Amendment grounds, the violating party must be a government actor. Because DTC companies are private entities and not government actors, the aggrieved consumer cannot sue the company on Fourth Amendment grounds. Assuming the consumer has the ability to sue the government on Fourth Amendment grounds for seizing their DNA, the third-party doctrine is likely the toughest hurdle to overcome and the primary reason legislative action is preferred. An individual gives up Fourth Amendment protections once he or she shares personal information to a third party. This standard will hold true "even if the information is revealed on the assumption that it will be used only for a limited purpose."[244] Accordingly, once a consumer swabs the inside of his cheek and mails the test tube back to the testing company, he has lost any privacy rights he may have had, and so have his family members. The Court has stepped away from its strict adherence to this standard in *Carpenter*, identifying that individuals do not abandon all expectations of privacy simply "by venturing into the public sphere."[245] However, the Court specified that the decision in *Carpenter* is a rare one, and the "government will be able to use subpoenas to acquire records in the overwhelming majority of investigations."[246] Even if the narrow standard carved out in *Carpenter* was applicable to the current issue, it would only extend to the individual consumer who submits the DNA initially.

Moreover, suing private companies for unauthorized disclosure is futile due to the signed informed consent agreements, which typically includes waiving any rights to the surrendered DNA, likely releasing any liability on behalf of the company.

The use of genetic information held by DTC genetic testing companies by law enforcement involves issues concerning who can sue, who can be sued, and on what grounds. The foregoing examination of Fourth Amendment jurisprudence highlights the difficulties of using a constitutional avenue to achieve genetic privacy protections. Thus, legislative action is necessary to (1) require DTC ancestry and genealogy companies to adopt an automatic "opt-out" policy for consumers; and (2) prohibit DTC companies from disclosing familial information.

---

244 United States v. Miller, 425 U.S. 435, 443 (1976).

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

246 *Id.* at 2222.

IV. PROPOSED SOLUTION

Legislation aimed at the regulation of private genetic information is unitary in nature, and specific to the individual. Regulation governing genetic testing in the clinical setting does not apply to most DTC companies because most do not provide health related tests. This is particularly worrisome because the companies are left to self-regulate and their policies fail to adequately inform consumers on what they are giving up, what data will be retained, with whom it might be shared, and how family members may be implicated. While some state laws may authorize a private right of action against such companies, these efforts are stunted by the policies signed by the consumer giving up rights to the surrendered DNA.

A. New Federal Legislation is the Proper Avenue for Addressing Genetic Privacy Issues

The Interim Policy introduced by the DOJ provides a great starting point for Congress to expand upon. The Policy identifies how investigation is to be conducted, when the use of private DTC databases may be used, and what happens to the genetic material after the investigation is over. The Policy also provides limitations on the types of crimes that may be investigated and the purposes for which the genetic material may be used. However, the DOJ Policy is not expansive enough. It only applies to federal law enforcement agencies and state agencies that receive funding from the federal government, leaving other state and local agencies free to utilize the investigation technique as they see fit. Further, the Policy does not require warrants or call for any kind of judicial oversight but rather places that responsibility with the prosecutors. The adopted Policy was not subject to Notice and Comment by the public, and thus, may be changed at any time. Lastly, and most importantly, the Policy does not confer upon the public any substantive or procedural rights or benefits enforceable at law. Although there is an expectation that the DOJ will comply with the guidelines, there is no remedy if they do not.

In order to fully account for the interests of all American citizens, it is not enough to only provide notice to consumers or implement procedural safeguards that protect the consumer. The problems can be reconciled with legislation that requires all DTC companies to adopt the "opt-out" policy and additionally ban disclosure of familial data to law enforcement by the company. Congress has the power to address these issues by way of the Commerce Clause.[247] DTC genealogy companies regularly engage in interstate commerce, and thus, are within the purview of Congress.

---

[247] CONST. art. I, Sec. 8, cl. 3.

B. The Proposed Law

Crime prevention and public safety are understandably compelling governmental interests, and equally obvious is the importance of civil liberties and privacy rights of the public. In order to balance these competing values, Congressional action is necessary. First, Congress should implement legislation requiring DTC ancestry and genealogy companies to adopt the "opt-in" feature similar to GEDmatch, i.e., all consumers are automatically opted out of sharing their genetic information with law enforcement unless they specifically choose to opt-in. This will ensure that people who do not read terms and conditions policies do not accidentally share their genetic information with law enforcement agencies. Second, Congress should forbid DTC companies from sharing familial information with law enforcement agencies. In effect, the only information that the company will be able to share with the agency would be exact matches. This will account for privacy interests of relatives who did not consent to the sharing of their DNA with law enforcement.

Allowing government officials warrantless access to private DNA banks expands the net of those subject to intrusion by the government. A DNA bank's ability to store genetic information indefinitely, coupled with the quantity of profiles stored[248] could potentially allow for unqualified, warrantless surveillance of virtually every single person. This proposed legislation will supplement the Policy established by the DOJ by giving citizens a choice as to how their personal information may be shared. While it will significantly decrease the amount of information available to law enforcement, it will also protect individuals from being surveilled, questioned, and investigated simply because a potentially unknown relative may have committed a crime at some point in their lifetime.

---

[248] As of March 2018, NDIS contains more than 13 million offender profiles, more than 3 million arrestee profiles, and more than 840 forensic profiles. GEDmatch contains 929,000 profiles.

V. CONCLUSION

Commenting on society's expectations concerning surveillance, Justice Scalia remarked, "Society's expectation has been that law enforcement agents and others would not—and indeed in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period of time."[249] This expectation against surreptitious monitoring logically extends to DNA information because such information can be retained indefinitely—after the purpose for which it was submitted has been completed—and may go on to implicate the voluntary submitter or a relative.

Genetic information privacy is becoming more essential and technology is growing rapidly. Federal and state governments' reluctance to protect that which is most fundamentally ours is becoming more important now than ever before. Allowing law enforcement unfettered access to massive private databases containing an incredible amount of exploitable, personal information is a form of surveillance that should only be allowed in fictional dystopian novels.

The Constitution protects all Americans' reasonable expectations of privacy. DNA is highly sensitive and contains inextricably personal information that should not be accessible by government officials, absent probable cause. A government with unlimited access to all personal information is a government with too much power.

---

[249] United States v. Jones, 565 U.S. 400, 430 (2012).