NOTES

FORENSIC GENEALOGY: THE BENEFITS, THE RISKS, AND THE IMMEDIATE NEED FOR LEGISLATIVE INTERVENTION

HALLIE P. GILLAM*

INTRODUCTION 617
I. BACKGROUND: WHAT IS FORENSIC GENEALOGY AND WHO ARE THE MAJOR PLAYERS IN THE FIELD 619
A. Player One: Direct to Consumer Genetic Testing (DTCs) ... 620
B. Player Two: GEDmatch 623
C. Player Three: Law Enforcement 624
II. ETHICAL AND LEGAL PROBLEMS WITH FORENSIC GENEALOGY 625
A. Informed Consent and Privacy 625
B. Lack of Regulation Leading to Misuse by Law Enforcement 629
1. *Mistake* 630
2. *Risk of Increased Discrimination* 631
III. WHY THE CONSTITUTION FAILS TO PROTECT GENETIC PRIVACY: THE FOURTH AMENDMENT AND THIRD-PARTY DOCTRINE 632
IV. REGULATORY MEASURES THAT CONGRESS SHOULD ADOPT AND HOW THEY AMELIORATE ETHICAL AND PRIVACY CONCERNS .. 635
A. Expand the DOJ's Forensic Genealogy Interim Policy into a National Model 636
B. Criminalize DNA Theft 636
C. Congress Should Prescribe Offense Types, Familial Proximity Limits, and the Obligations of Genetic Information Holders 638
D. Require Law Enforcement to Obtain a Warrant 639
E. Require DTCs and Genetic Databases to Include Opt-In Provisions and Demand Written Informed Consent 640
F. In the Alternative, Congress Could Implement Industry Standards to Better Regulate the Area of Forensic Genealogy .. 641
CONCLUSION 643

INTRODUCTION

In 2019, a mother and a daughter reunited after fifty-two years with the help of DNA testing.[1] Erin Chatterton, an Ohio woman who never knew her biological parents, received an AncestryDNA kit as a birthday gift and decided to take the test out of curiosity.[2] Halfway across the country in San Diego, California, Lisa Raessner took the same test in an effort to piece together missing links in her family tree. Chatterton and Raessner got a match soon after.[3] After reaching out to family for answers about the possible link between the two women, an unexpected secret shocked the family: Raessner's step-mother revealed that she had given birth to a child that she had with Raessner's father before they were married and was forced to give her up for adoption after being thrown out of her home by her religious family.[4] A DNA test confirmed that Chatterton was, indeed, the daughter of Raessner's step-mother, Karen Leslie.[5] The mother and daughter reunited in San Diego; Leslie was given a daughter, and Chatterton was given answers to a decades-old mystery, a biological mother, and two new sisters.

At the same time, and in the same state, the apprehension of Joseph James DeAngelo Jr.—better known as the Golden State Killer—was sending shockwaves throughout the country.[6] The Golden State Killer terrorized the state of California throughout the 1970s and 1980s, and is considered to be one of America's most prolific serial killers.[7] Law enforcement suspects that he is responsible for committing sixty home invasions, fifty rapes, and thirteen murders.[8] Though his criminal activity ceased in the 1980s, police were not able to identify him.[9] Last year,

---

* Juris Doctor candidate, Belmont University College of Law, 2021. I want to thank all my Professors, especially Professors Jeffrey Usman and Elizabeth Usman, for their guidance in developing this note. Additionally, I am so thankful for the entire editorial team for their valuable feedback. Lastly, thank you to my family and friends for your love and support throughout my law school career.

1. Stacy Chen, *DNA tests prompt family reunion 52 years in the making*, ABC NEWS (Jan. 12, 2019), https://abcnews.go.com/US/dna-tests-prompt-family-reunion-52-years-making/story?id=60311558 [https://perma.cc/9YPN-ACCZ].
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. Paige St. John et al., *Mapping the Golden State Killer*, L.A. TIMES (June 11, 2019), https://www.latimes.com/projects/man-in-the-window-crime- map-golden-state-killer-serial/ [https://perma.cc/6WP9-AKT9].
7. *Id.*
8. *Id.*
9. Breeana 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 [https://perma.cc/9PNQ-VPDN].

however, police arrested DeAngelo Jr. and charged him as the Golden State Killer.[10] Law enforcement was able to solve the case after his DNA sample was uploaded to GEDmatch—a public DNA database—which found a match in a distant relative.[11] Investigators then used genealogical research methods to reverse-engineer a family tree, leading to DeAngelo Jr. After police identified him as a suspect, they took a DNA sample from his trash and compared it to the DNA found at the crime scenes.[12] After almost fifty years, the mystery of the Golden State Killer was solved.

DNA has changed the lives of millions of people across the country. Many, like Chatterton and Leslie, have found long-lost relatives and answers to questions about their families' history. Others, like the families of the Golden State Killer's victims, have been given justice and peace that they believed may never come. Yet, increased use of genetic information comes with disadvantages as well. Mainly, it poses risks to individual privacy due to a lack of federal regulation. The purpose of this piece is to offer background, concerns, and legislative recommendations in regards to the use of genetic information. While the sole focus of this Note is to address its use of genetic information by law enforcement, I offer considerations about its uses (and potential uses) by other parties as well in an effort to suggest a regulatory model that addresses a wide array of risks.

In Section I, this Note discusses forensic genealogy at large: what it is, its increased prevalence in American society, and who the major players are in the industry. In Section II, this Note addresses privacy and ethical concerns surrounding its use, primarily in criminal investigations. Primarily, these include lack of informed consent by consumers and misuse by law enforcement. In Section III, I examine constitutional concerns, particularly in respect to the Fourth Amendment's third-party doctrine. I explain why there is a lack of Fourth Amendment protection, using cases to define the narrow scope of protection over genetic information as afforded by the Supreme Court. Finally, in Section IV, I offer feasible regulations that Congress could implement in order to legislate the field of forensic genealogy and genetic privacy at large. Specifically, I suggest transforming the Department of Justice's forensic genealogy interim policy into the national model, expanding it and adding safeguards to further procure individuals' privacy while balancing society's interest in justice.

10. St. John et al., *supra* note 6.

11. Jocelyn Kaiser, *New federal rules limit police searches of family tree DNA databases*, SCI. MAG. (Sept. 25, 2019), https://www.sciencemag.org/news/2019/09/new-federal-rules-limit-police-searches-family-tree-dna-databases [https://perma.cc/SP5J-3B6D].

12. Hare & Taoushiani, *supra* note 9.

I. BACKGROUND: WHAT IS FORENSIC GENEALOGY AND WHO ARE THE MAJOR PLAYERS IN THE FIELD

Forensic Genealogy is the process of using DNA matches to reverse-engineer a family tree.[13] A DNA sample, usually saliva, is submitted to a DNA database, like Ancestry.com, 23andMe, or FamilyTreeDNA.[14] This results in matches of individuals with similar DNA.[15] "Family trees are developed for individuals as close or closer than third or fourth cousins, with an eye to where disparate branches of the family tree cross, indicating a family where both paternal and maternal lines combine in a single family."[16] After matches are identified, genealogical investigation is required to construct the entire family tree. Common resources used by genealogists are "census records, vital records, newspaper archives, public 'people search' databases, public social media data, and public family trees."[17] Occasionally, researchers identify two potential DNA matches for a single sample. In this case, researchers perform descendancy research to trace the descendants of each set of ancestors to locate an intersection between them.[18]

Direct to Consumer genetic testing is a profitable and expanding industry in the United States. A study suggests that it is possible to identify a match from a single third cousin, identifying his or her sex, location within 100 miles, and approximate age within five years.[19] Additionally, a report conducted by Science Magazine claims that "[i]f you're white, live in the United States, and a distant relative has uploaded their DNA to a public ancestry database, there's a good chance an internet sleuth can identify you from a DNA sample left somewhere."[20] This ability could potentially identify up to sixty percent of white Americans from a single DNA sample.[21] Because of the mounting use by consumers, and the developments in understanding about genealogy, we as a society are likely a few years away from being able to identify anyone and everyone.[22]

---

13. Colleen Fitzpatrick & Dee Dee King, *Forensic Genealogy—Dead Men Do Tell Tales*, RECORD CLICK PROF'L GENEALOGISTS (Mar. 9, 2020), https://www.recordclick.com/forensic-genealogy-dead-men-do-tell-tales/ [https://perma.cc/UCK3-MRJ4].

14. Ray A. Wickenheiser, *Forensic Genealogy, Bioethics and the Golden State Killer Case*, 1 FORENSIC SCI. INT'L: SYNERGY 114, 116 (2019).

15. *Id.* at 118.

16. *Id.*

17. Ellen M. Greytak et al., *Genetic Genealogy for Cold Cases and Active Investigations*, 299 FORENSIC SCI. INT'L 103, 110 (2019).

18. *Id.*

19. *Id.* at 108.

20. Jocelyn Kaiser, *We will find you: DNA search used to nab Golden State Killer can home in on about 60% of white Americans*, SCI. MAG. (Oct. 11, 2018), https://www.sciencemag.org/news/2018/10/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white [https://perma.cc/L6CC-9RC6].

21. *Id.*

22. *Id.*

Forensic genealogy is relatively new, but it is gaining popularity both as a way of identifying ancestors and of solving criminal cases.[23] With new technology, however, comes a need for regulation to address ethical concerns associated with the practice. While citizens and the government alike appreciate convicting serial killers, rapists, and other violent criminals, there are ethical concerns that deserve adequate consideration.[24] As the Sacramento County District Attorney explained, "[i]t is probably one of the greatest revolutions, at least I would say, in my lifetime as a prosecutor . . . [b]ut it is a difficult, evolving topic because there are privacy interests at stake in an area that's unregulated."[25] Privacy concerns, however, are just one of several concerns at play within this new era of genealogical technology.

A. Player One: Direct to Consumer Genetic Testing (DTCs)

Direct to Consumer ("DTC") genetic testing markets directly to customers.[26] Customers submit a DNA sample and receive results about their ancestry directly through a secured website or a report.[27] The DTC genetic testing industry has skyrocketed in the last few years, with more than twenty-six million people having taken at-home DNA samples at a price as low as fifty-nine dollars.[28] Popular DTC providers are Ancestry.com, 23andMe, FamilyTreeDNA, and MyHeritage.[29]

The terms and conditions associated with these providers vary slightly, but are relatively similar in many ways. Ancestry.com, the largest DTC provider with more than fifteen million DNA samples in its system, requires a consumer to be eighteen years old or over, but also allows a parent with full legal custody to send in his or her child's sample.[30] A vial of saliva is submitted to the company, with which the company develops an

23. Paige St. John, *DNA genealogical databases are a gold mine for police, but with few rules and little transparency*, L.A. TIMES (Nov. 24, 2019), https://www.latimes.com/california/story/2019-11-24/law-enforcement-dna-crime-cases-privacy [https://perma.cc/69G5-CKCM].

24. Benjamin Berkman, *The Questionable Ethics of Expanding Forensic DNA Testing*, PAC. STANDARD (Mar. 21, 2019), http://www.psmag.com/social-justice/the-ethical-questions-about-expanded-dna-testing [https://perma.cc/6EW9-FLUG].

25. St. John, *supra* note 23.

26. U.S. Nat'l Libr. of Med., *What is direct-to-consumer genetic testing?*, GENETIC HOME REFERENCE (Nov. 26, 2019), https://ghr.nlm.nih.gov/primer/dtcgenetictesting/directtoconsumer [https://perma.cc/QYG6-4QXS].

27. *Id.*

28. Antonio Regalado, *More than 26 million people have taken an at- home ancestry test*, MIT TECH. REV. (Feb. 11, 2019), https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/ [https://perma.cc/VQ57-AYT2].

29. *Id.*

30. Greytak et al., *supra* note 17.

ancestry report.[31] Ancestry requires "explicit consent" from the individual providing the DNA sample.[32] The company's approach to its practice is that the individual owns their own data and declares such at the beginning of the terms and conditions.[33] Consumers, by submitting DNA samples, grant the company a license to their data, which can be revoked when consumers request that their data be destroyed and deleted.[34] Ancestry makes clear that they will not share consumers' information with employers, insurance providers, or marketers without obtaining consent.[35] The privacy statement also states that it will not cooperate with law enforcement absent a court order or subpoena and will inform the consumer with advance notice unless otherwise prohibited by law.[36] Additionally, in regards to law enforcement, Ancestry produces a yearly transparency report, in which it lists the number of valid law enforcement requests it received.[37] In 2018, Ancestry received ten requests and provided information in response to seven.[38] Each request involved investigations into credit card misuse, fraud, and identity theft.[39] However, Ancestry received no valid request for genetic information—only having provided user information—and stated that it does not disclose such information to law enforcement.[40]

23andMe, like Ancestry, requires an individual to submit a sample of their saliva or a sample for someone over whom he or she has legal authority.[41] 23andMe states on its website that it "chooses to use all practical legal and administrative resources to resist requests from law enforcement, and [it does] not share customer data with any public databases, or with entities that may increase the risk of law enforcement access."[42] If law enforcement presents a court order, subpoena, or search warrant for genetic or user information, however, it may be required by law to comply.[43] 23andMe also produces a transparency report, though less

---

31. *Ancestry Terms and Conditions*, ANC., https://www.ancestry.com/cs/legal/termsandconditions [https://perma.cc/XL7S-2WC2].

32. *Id.*

33. *Id.*

34. Eric Heath, *Setting the Record Straight: Ancestry and Your DNA*, ANC. (May 21, 2017), https://blogs.ancestry.com/ancestry/2017/05/21/setting-the-record-straight-ancestry-and-your-dna/ [https://perma.cc/SZN8-NPMV].

35. *Id.*

36. *Your Privacy*, ANC., https://www.ancestry.com/cs/legal/privacystatement [https://perma.cc/YCD6-JTSR].

37. *Id.*

38. *Ancestry 2018 Transparency Report*, ANC., https://www.ancestry.com/cs/transparency-2018 [https://perma.cc/GAF6-HD5N] (last visited Dec. 13, 2021).

39. *Id.*

40. *Id.*

41. *Terms of Service*, 23ANDME (Sept. 30, 2019), https://www.23andme.com/about/tos/ [https://perma.cc/WFM4-ZNV7].

42. *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide/ [https://perma.cc/ZXU3-UV5P].

43. *Id.*

frequently than Ancestry, and reported in 2019 that—of seven government requests for data—it provided data in response to none of them.[44]

FamilyTreeDNA's kits consist of cotton swabs an individual may use to collect his or her DNA and that are submitted to the company along with a signed consent form.[45] The company also accepts blood cards, wherein participants can deposit a small amount of blood onto a secure slip.[46] FamilyTreeDNA states that it will cooperate with law enforcement officers, but requires them to request to submit a sample or genetic file to the database.[47] Permission is only granted to identify a perpetrator of a violent crime, such as homicide, sexual assault, or abduction, and also to identify the remains of a deceased individual.[48] FamilyTreeDNA does not produce a transparency report, but has stated that it is working toward publishing them.[49]

MyHeritage, which operates out of Europe,[50] requires customers to submit a cheek swab.[51] The terms and conditions state that by doing so, the individual affirms that the sample is his or her own, or that of a child over whom they are a legal guardian.[52] The terms also state that a third-party sample may be submitted for whom the individual has obtained legal authorization to provide his or her DNA.[53] In regards to cooperation with law enforcement, the company provides that "using the DNA Services for law enforcement purposes, forensic examinations, criminal investigations, 'cold case' investigations, identification of unknown deceased people, location of relatives of deceased people using cadaver DNA, and/or all similar purposes, is strictly prohibited, unless a court order is obtained."[54] The company does not produce a transparency report.[55]

Because of its novelty, complexities, and competing interests, the DTC market is not highly regulated in the United States. Author Elizabeth

---

44. *Transparency Report*, 23ANDME, https://www.23andme.com/transparency-report/ [https://perma.cc/29S3-DS39] (last visited Dec. 13, 2021).

45. *DNA Test Kit Instructions*, FAMILYTREEDNA, https://www.learn.familytreedna.com/testing-process/dna-test-kit-instructions/ [https://perma.cc/T6DJ-NSB9] (last visited Dec. 13, 2021).

46. *FamilyTreeDNA Learning Center*, FAMILYTREEDNA, https://learn.familytreedna.com/ftdna/forensic-samples/ [https://perma.cc/3BR6-4L8S] (last visited Dec. 13, 2021).

47. *FamilyTreeDNA Law Enforcement Guide*, FAMILYTREEDNA, https://www.familytreedna.com/legal/law-enforcement-guide [https://perma.cc/Q6LK-XEWK] (last visited Dec. 13, 2021).

48. *Id.*

49. *Id.*

50. Regalado, *supra* note 28.

51. *How Does DNA Testing Work*?, MYHERITAGE, https://www.myheritage.com/dna [https://perma.cc/M3YE-HKJG] (last visited Dec. 13, 2021).

52. *Terms and Conditions*, MYHERITAGE, https://www.myheritage.com/terms-and-conditions [https://perma.cc/3GAP-6RFS] (last visited Dec. 13, 2021).

53. *Id.*

54. *Id.*

55. *Id.* (showing that there is an omission of transparency report).

E. Jon describes the DTC industry as the "wild west."[56] In 2010, the U.S. Food and Drug Administration ("FDA") attempted briefly to regulate the industry when it notified a company that its genetic testing kit "appeared to meet the definition of a medical device" under the Food, Drug, and Cosmetic Act.[57] Meeting this definition seemingly provided the FDA with jurisdiction to regulate the kit and others like it. Using its "enforcement discretion," however, it chose not to regulate the market used for ancestry purposes.[58] However, the FDA does provide information about DTC testing on its website, clarifying that no test is one-hundred percent accurate.[59] It also granted market clearance to 23andMe to conduct health screening.[60] Again, however, they provide no serious regulations on DTC genetic testing.[61] The Federal Trade Commission similarly does not provide any regulation or oversight of laboratories used by DTC companies for ancestry purposes.[62]

The Centers for Medicare and Medicaid Services ("CMS") is, peculiarly, the federal agency most involved in regulating DTC testing.[63] CMS oversees the laboratories providing testing services under the Clinical Laboratory Improvement Amendments, though its regulatory authority extends only to analytical—but not clinical—validity.[64] Analytical validity identifies the presence of a genetic variation, while clinical validity addresses whether the variation correlates to a specific disease or condition.[65] Though a seemingly meaningless discrepancy, it demonstrates the significant lack of regulatory authority administered by CMS.[66]

B. Player Two: GEDmatch

GEDmatch, the website used to solve the Golden State Killer case, is not a DTC provider because it does not receive direct samples of DNA from consumers. Rather, it is a public platform through which consumers may upload their DTC-generated DNA results to compare with other individuals.[67] After the apprehension of the Golden State Killer, GEDmatch

---

56. Elizabeth E. Joh, *DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing*, 91 B.U. L. REV. 665, 675 (2011).

57. Justice Ming W. Chin et al., Forensic DNA Evidence: Science and the Law § 13:15 (2021).

58. Joh, *supra* note 56.

59. *Direct-To-Consumer Tests*, FDA, https://www.fda.gov/medical-devices/vitro-diagnostics/direct-consumer-tests [https://perma.cc/8K8P-TTJX].

60. *Id.*

61. *Id.*

62. Joh, *supra* note 56, at 674.

63. *Id.* at 675.

64. *Id.*

65. *Id.*

66. *Id.*

67. *Tools for DNA and Genealogy Research*, GEDMATCH, https://www.gedmatch.com/login1.php [https://perma.cc/CBQ6-98RK] (last visited Dec. 13, 2021).

decided to allow law enforcement to use the site.[68] It informed its users with the following statement:

> While the database was created for genealogical research, it is important that GEDmatch participants understand the possible use of their DNA, including identification of relatives that have committed crimes or were victims of crimes. If you are concerned about non-genealogical uses of your DNA, you should not upload your DNA to the database and/or you should remove DNA that has already been uploaded.[69]

The announcement was followed by an influx of participants.[70] GEDmatch is forthcoming with its cooperation with law enforcement, stating in its Terms of Service and Privacy Policy that a participant's DNA may be compared to that of DNA obtained by law enforcement to identify a perpetrator of a violent crime or that of a deceased individual.[71] Additionally, the company partnered with Parabon, a company that, on a weekly basis, compares DNA uploaded to GEDmatch to DNA provided by law enforcement in order to solve cases.[72]

C. Player Three: Law Enforcement

Since the Golden State Killer's arrest, more than thirty murderers, rapists, and victim's bodies have been identified through forensic genealogy,[73] including the NorCal rapist, a man who murdered an eight-year-old girl in 1988.[74] Some sources report up to sixty-six of such cases.[75]

June of 2019 saw the first case solved using forensic genealogy.[76] After a thirty-year investigation of hundreds of leads, William Earl Talbott was convicted and found guilty of the murder of a couple in British

68. Greytak et al., *supra* note 17, at 106.
69. *Id.*
70. *Id.* at 107.
71. *Terms of Service and Privacy Policy*, GEDMATCH (Dec. 9, 2019), https://www.gedmatch.com/terms-of-service-privacy-policy [https://perma.cc/TPQ8-DAAJ].
72. Greytak et al., *supra* note 17, at 107.
73. Regalado, *supra* note 28.
74. Greytak et al., *supra* note 17, at 104.
75. St. John, *supra* note 23.
76. *SeaTac Man Convicted of 1987 Murders of Canadian Couple After DNA Evidence Linked Him to Case,* SEATTLE TIMES (June 28, 2019), https://www.seattletimes.com/seattle-news/crime/seatac-man-convicted-of-1987-murders-of-canadian-couple-after-dna-evidence-linked-him-to-case/#:~:text=Science-,SeaTac%20man%20convicted%20of%201987%20murders%20of%20Canadian%20couple,evidence%20linked%20him%20to%20case&text=A%20Snohomish%20County%20jury%20deliberated,%2Dyear%2Dold%20Jay%20Cook [https://perma.cc/R6JJ-AX8X].

Columbia.[77] Using the Parabon laboratories, a Snohomish County Sheriff's detective reverse-engineered a family tree, leading to two unrelated second cousins and, eventually, to Talbott.[78] The DNA data from Parabon was matched with a sample taken from a discarded cup, and Talbott was subsequently arrested and convicted.[79]

Forensic genealogy can also be used to exonerate wrongfully-convicted individuals, as exemplified by the case of Christopher Tapp.[80] In 1996, Tapp was convicted of a rape and murder of an eighteen-year-old.[81] Many advocates for Tapp over the years have suggested that his confession was coerced, but his name was not cleared until 2019 when an Idaho judge dismissed all charges against him after forensic genealogy confirmed that the DNA evidence from the crime scene was not his.[82] From a criminal justice standpoint, the benefits of using forensic genealogy are immeasurable. Both convictions and exonerations can be pursued with much more accuracy, and wrongful convictions are much less likely to take place when using these methods.

II. ETHICAL AND LEGAL PROBLEMS WITH FORENSIC GENEALOGY

A. Informed Consent and Privacy

Informed consent is defined as "an agreement to do something or to allow something to happen, made with complete knowledge of all relevant facts, such as the risks involved or any available alternatives."[83] In reference to forensic genealogy, consumers—even those who have signed a consent form—often remain unaware of the potential implications and repercussions of using a DTC company for ancestry purposes.[84] The head of ethics of genetics and new technologies at the National Institute of Health's Department of Bioethics, Benjamin Berkman, stated, "Genealogy is typically done for entertainment purposes…People may not realize uploading their DNA could be responsible for a cousin's arrest as well."[85]

77. *Id.*
78. *Id.*
79. *Id.*
80. Mia Armstrong, *In an Apparent First, Genetic Genealogy Aids a Wrongful Conviction Case*, THE MARSHALL PROJECT (July 17, 2019), https://www.themarshallproject.org/2019/07/16/in-an-apparent-first-genetic-genealogy-aids-a-wrongful-conviction-case [https://perma.cc/3U4G-AX6T].
81. *Id.*
82. *Id.*
83. *Informed Consent*, LEGAL INFO. INST. (July 5, 2021), https://www.law.cornell.edu/wex/informed_consent [https://perma.cc/U5PC-PM8U].
84. Solana Lund, *Ethical Implications of Forensic Genealogy in Criminal Cases*, 13 J. BUS. ENTREPRENEURSHIP & L. 185, 197 (2020).
85. Carolyn Crist, *Experts Outline Ethics Issues with Use of Genealogy DNA to Solve Crimes*, REUTERS (June 1, 2018), https://www.reuters.com/article/us-health-ethics-genealogy

Terms of Service agreements do not explain the implications of submitting DNA, and navigating legalese is often not possible for the average person.[86] Individuals, by submitting their DNA, may contribute to solving cold cases, as was the case with a woman in Washington State whose information on GEDmatch led to the arrest of a distant relative.[87] While, after his arrest, she stated that she was "OK" with her DNA being used in such a manner, she was unaware of that possibility.[88]

Studies have also been conducted that highlight issues regarding whether or not DNA submitters actually gave any consent to DTCs.[89] Though the Terms and Conditions of most DTCs require consent—or implied consent—with the submission of their DNA, there is little done to ensure that this requirement is actually being met by consumers. The lack of regulation deters DTCs from doing so as well.[90] A report by New Scientist found that "genome hacking" was, in fact, very easy to do.[91] A journalist "collect[ed] his colleague's saliva from a cup (with his consent)…[and had] one company extract the DNA, another amplify the sample to create enough DNA for analysis, and yet another analyze the DNA for any medical predispositions."[92] He also "successfully submitted a cheek swab with his colleague's DNA for analysis."[93] None of the companies took steps to ensure that the claimed DNA was actually his own. Conducting this type of "genome hacking" is as simple as forging a signature or checking a box.[94]

Additionally, individuals that submit their DNA data to various databases may not know who may access their information. There is a regulatory process, however, for an individual who participates in a federal research study or clinical trial that generates DNA data.[95] The 21st Century Cures Act (2016) and the U.S. Common Rule require that the genetic donor is provided with a certificate of confidentiality and mandate that he or she is informed of how the data may be shared, respectively.[96] Thus, legal recourse can be taken if that information is somehow illegally obtained, and

---

-dna/experts-outline-ethics-issues-with-use-of-genealogy-dna-to-solve-crimes-idUSKCN1IX5O6 [https://perma.cc/EG4H-BNDA].

86. *Id.*

87. Sarah Zhang, *A DNA Company Wants You to Help Catch Criminals*, THE ATLANTIC (Mar. 29, 2019), https://www.theatlantic.com/science/archive/2019/03/a-dna-company-wants- your-dna-to-catch-criminals/586120/.

88. *Id*.

89. Lund, *supra* note 84.

90. Joh, *supra* note 56, at 677–78.

91. *Id.* at 678.

92. *Id.*

93. *Id.*

94. *Id.*

95. Megan Molteni, *The U.S. Urgently Needs New Genetic Privacy Laws*, WIRED (May 1, 2019), https://www.wired.com/story/the-us-urgently-needs-new-genetic-privacy-laws/ [https://perma.cc/8MWL-7C2S].

96. *Id.*

the information would be inadmissible in court.[97] However, if the individual then wants to add the genetic information to an electronic health record, making it available to his or her doctor, it becomes governed by the Health Insurance Portability and Accountability Act ("HIPAA").[98] Under HIPAA, law enforcement agencies are entitled to access personal genetic information without a warrant if the individual becomes a victim or suspect of a criminal investigation.[99] Because such personal genetic information is in the health record, an insurance provider may also access it.[100] While Congress passed the Genetic Nondiscrimination Act ("GINA") in 2008 to prevent health insurers from denying coverage or increasing prices based on genetic predispositions, it does not apply to long-term-care insurance, life insurance, or disability insurance.[101] And, while the Affordable Care Act ("ACA") protects individuals with pre-existing health conditions against health insurance discrimination, the Trump administration actively worked to peel back this provision, and other provisions, of the act.[102]

However, none of the aforementioned laws—the Common Rule, GINA, nor the ACA—provide protections against other potential uses of DNA data.[103] In every state except California, it is legal for a condominium association in a retirement community to require a DNA sample from its residents confirming that they are not genetically predisposed to Alzheimer's.[104] Even schools could legally require DNA tests for admissions or to reject children with certain genetic predispositions.[105] While this may seem unfathomable to many, this scenario took place in California, when a sixth grader was kicked out of school because of his genetic markers for cystic fibrosis.[106] Michelle Lewis, a pediatrician, attorney, and researcher at Johns Hopkins Berman Institute of Bioethics warns, "As we do more screening earlier and earlier in life, there's potential for misuse of information in ways that are harmful, that could potentially discourage parents from seeking genetic testing even if it's medically indicated."[107]

Surely, a consumer does not provide informed consent if they are unaware of the variety of institutions that may access their DNA. From law enforcement to health insurance providers to schools, the common

97. *Id.*
98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.*
102. *Id.*
103. *Id.*
104. *Id.*
105. Sarah Zang, *DNA Got a Kid Kicked Out of School—And It'll Happen Again*, WIRED (Feb. 1, 2016), https://www.wired.com/2016/02/schools-kicked-boy-based-dna/ [https://perma.cc/2YVV-X7FQ].
106. *Id.*
107. *Id.*

consumer of DTC DNA testing does not predict the ways in which genetic testing may be used. A concerning lack of regulations and laws surrounding this area mean that, if Congress does not take quick legislative action, a variety of different organizations and establishments may soon be able to partake in a sort of genetic discrimination.[108]

While considerations of informed consent and an understanding of the potential implications of forensic genealogy overlap with concerns about privacy, there are additional, separate issues that must also be addressed. Specifically, forensic genealogy raises important questions about expectations of privacy and abandoned property. Individuals leave discarded DNA everywhere they go: cups tossed into the trash, cigarettes thrown on the ground, hair follicles, and skin cells. "It is comparable to discarded or abandoned property . . . [and] legally analogous to trash."[109]

Importantly, regardless of what DTCs claim about their willingness to cooperate with law enforcement, there are no obstacles in place to keep them from doing so unbeknownst to consumers. For example, in 2019, FamilyTreeDNA worked secretly with the FBI and allowed them to search the entire database.[110] The company has faced no repercussions, and the company is now outwardly advertising its cooperation with law enforcement.[111] Additionally, while databases can currently be used only to transiently search for partial genetic matches, investigators with warrants may be able to access the entire database and hold on to a vast amount of genetic information in the foreseeable future.[112]

Lastly, in addition to individual privacy concerns, forensic genealogy also poses risks to other people's privacy as well. An individual's DNA information contains a significant amount of information about their relatives.[113] Thus, while some sites like GEDmatch explicitly warn participants of their willingness to cooperate with law enforcement and the possibility of their own DNA being used to help solve crimes, their relatives' information is also made publicly available, often without their knowledge.[114]

---

108. Molteni, *supra* note 95.

109. Lund, *supra* note 84, at 200.

110. Matthew Haag, *FamilyTreeDNA Admits to Sharing Genetic Data With F.B.I.*, N.Y. TIMES (Feb. 4, 2019), https://www.nytimes.com/2019/02/04/business/family-tree-dna-fbi.html [https://perma.cc/3PW8-AP8N].

111. *Id.*

112. Raehoon Jeong, *How Direct-to-Consumer Genetic Testing Services Led to the Capture of the Golden State Killer*, SITN BOS. (Sept. 2, 2018), http://sitn.hms.harvard.edu/flash/2018/direct-consumer-genetic-testing-services-led-capture-golden-state-killer/ [https://perma.cc/8YJR-4Q8W].

113. *Id.*

114. *Id.*

B. Lack of Regulation Leading to Misuse by Law Enforcement

In *Kyllo v. United States,* the Supreme Court established that law enforcement officers can use any technology in their investigations that is readily available to the public.[115] As previously mentioned, millions of consumers use genetic testing through DTCs, so law enforcement is able to enjoy the benefits of it as well. However, because nothing bars or regulates the use of forensic genealogy in criminal cases,[116] several issues have been identified concerning law enforcement's use of the technology.

In response to public unrest following the arrests of the Golden State Killer, the United States Department of Justice ("DOJ") implemented an interim policy on forensic genetic genealogical DNA analysis and searching ("FGGS") that went into effect on November 1, 2019.[117] In an effort to balance privacy interests and the benefits associated with law enforcement's use of FGGS, identify violent criminals, exonerate innocent suspects, and ensure justice, the DOJ prohibited information derived from FGGS from being uploaded and retained in the CODIS DNA Index, the governmental DNA database.[118] Additionally, the policy clarifies that no suspect can be arrested based solely on a genetic association.[119] An identified suspect's DNA must be compared to DNA found at the original crime scene.[120] The DOJ also set forth case criteria, restricting the use of these procedures to only identify perpetrators of unsolved homicides or sex crimes and unidentified remains of a suspected homicide victim.[121] Prosecutors may also use forensic genealogy when a substantial and ongoing threat to public safety or national security exists.[122] DTCs must now identify whether or not they cooperate with law enforcement through "explicit notice."[123]

The policy, however, only applies in four circumstances.[124] First, it applies to criminal investigations in which the DOJ has exclusive or concurrent jurisdiction of the crime and lawful custody of the forensic samples.[125] Second, it applies to any criminal investigation in which the DOJ provides funding to a federal, state, local, or tribal agency.[126] Third, the policy governs criminal investigations in which DOJ employees or

115. Kyllo v. United States, 533 U.S. 27, 33–35 (2001).
116. Joh, *supra* note 56, at 675.
117. U.S. DEP'T OF JUST., INTERIM POLICY: FORENSIC GENETIC GENEALOGICAL DNA ANALYSIS AND SEARCHING (2019), https://www.justice.gov/olp/page/file/1204386/download [https://perma.cc/8KE4-JVHE].
118. *Id.* at 3–4.
119. *Id.* at 4.
120. *Id.*
121. *Id.*
122. *Id.*
123. *Id.* at 6.
124. *Id.* at 2.
125. *Id.*
126. *Id.*

contractors conduct the genealogical research on leads generated through forensic genealogy.[127] Finally, it applies to any federal agency, unit of state, local, or tribal government that receives grants from the DOJ for the purpose of forensic genealogy.[128] Thus, the policy leaves many state and local law enforcement agencies absent of any regulation.

1. Mistake

Moreover, the FDA's warning of incorrect results that can occur in DNA tests and the DOJ's policy requiring an arrest to be made on more than a match are indicative of the reality of forensic genealogy: mistakes can happen. In *Inside the Cell: The Dark Side of Forensic DNA*, Professor Erin Murphy emphasizes that forensic DNA is not yet a perfect science.[129] She states, "there's a huge difference between taking a controlled DNA sample in a clinical setting, like a laboratory or a hospital, and testing DNA found at a crime scene . . . In the rough and tumble world of crime, DNA is going to be subject to all these conditions that make it much more difficult to get an accurate result."[130]

Additionally, genetic genealogy can be plagued by the same human biases that plague other aspects of law.[131] Close relatives, and even non-relatives, can be suspected or accused of a crime if care is not taken in interpreting the data.[132] A New Orleans filmmaker, for example, was suspected of raping and murdering a Ohio woman in 1996.[133] Using GEDmatch, law enforcement identified his father, which led them to identify him.[134] The filmmaker provided law enforcement with a DNA sample, which they spent the next month comparing to the DNA from the crime scene, leaving the young man to agonize over a potential unexplained match.[135] He was informed later that the DNA did not match.[136] While demanding someone to submit a DNA sample is not exactly a huge burden to bear, this example is indicative of the imperfections in forensic genealogy that infringe on innocent people's privacy and daily lives.

---

127. *Id.*
128. *Id.*
129. *Testing DNA: In her new book, Erin Murphy investigates how the criminal justice system misuses genetic identification,* N.Y.U. (Oct. 7, 2015), https://www.law.nyu.edu/news/ideas/Erin-Murphy-forensic-DNA [https://perma.cc/W3NZ-K6T3].
130. *Id.*
131. Nsikan Akpan, *Genetic genealogy can help solve cold cases. It can also accuse the wrong person,* PBS NEWS (Nov. 7, 2019), https://www.pbs.org/newshour/science/genetic-genealogy-can-help-solve-cold-cases-it-can-also-accuse-the-wrong-person [https://perma.cc/T72N-FMXS].
132. *Id.*
133. *Id.*
134. *Id.*
135. *Id.*
136. *Id.*

The DNA used most by law enforcement is called autosomal genealogy, consisting of 700,000 letters.[137] These letters can be misinterpreted, and DTC reports can contain errors. A small but critical 2018 study found that up to forty-percent of the SNPs—subtle variations in the letters—can lead to a false positive match in ancestry.[138] The results were later reaffirmed by a 2019 study.[139] Additionally, autosomal genealogy cannot distinguish between siblings because their DNA is too similar.[140] Because genetic genealogy can be used only to create a family tree, a crime committed by an individual's brother can lead to a wrongful conviction.[141] This is, of course, further complicated when family structures are more complex, involving illegitimate children and adoption.

2. Risk of Increased Discrimination

According to Benjamin Berkman of the National Human Genome Research Institute, the future developments in forensic genealogy also justify concern.[142] Another technique rising alongside of genetic genealogy, known as DNA phenotyping, may lead to discrimination in the criminal justice system—more than exists already.[143] DNA phenotyping involves creating a picture of an individual based on DNA. Eye color, hair color, skin color, and face shape will be available for investigators to narrow down their searches of suspects and Jane Does.[144] "The science there is much less well-developed," Berkman said, explaining that great caution should be involved in targeting people.[145] In Germany, for example, DNA phenotyping indicated that a murder suspect was a part of an ethnic minority.[146] Law enforcement proceeded to harass members of the minority group before discovering that the sample was contaminated.[147]

The accuracy of DNA phenotyping varies depending on the trait.[148] It can, for instance, predict brown eyes with ninety percent accuracy, but cannot pinpoint grey colors.[149] Additionally, very dark and very light skin colors can be identified with precision, but everything in between cannot be

137. *Id.*
138. *Id.*
139. *Id.*
140. *Id.*
141. *Id.*
142. *Id.*
143. *Id.*
144. *Id.*
145. *Id.*
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*

predicted with much accuracy.[150] Moreover, DNA phenotyping requires a degree of human interpretation, allowing for bias and discrimination.[151]

Forensic genealogy is unquestionably a helpful tool for law enforcement, allowing them to close cold cases, determine the identities of deceased individuals, and exonerate innocent suspects. However, the lack of regulation and legislation in this area—especially in jurisdictions outside of the DOJ's FGGS policy—is vulnerable to many problems. Like with most technology, the results are not always accurate in DNA sampling. Mistakes can be made in laboratories or when interpreting the results. Messy crime scenes may also lead to contaminated DNA. Additionally, the evolving use of DNA phenotyping may lead to increased discrimination in a criminal justice system already plagued by it.

III. WHY THE CONSTITUTION FAILS TO PROTECT GENETIC PRIVACY: THE FOURTH AMENDMENT AND THIRD-PARTY DOCTRINE

In 1967, the Supreme Court held in *Katz v. United States* that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[152] The Court also explained in *Smith v. Maryland* that "a person has no legitimate expectation of privacy in information [that] he voluntarily turns over to third parties."[153] This principle has become known as the third-party doctrine.[154] The third-party doctrine has enabled the government to investigate in a society where information from each individual is being shared at all times through many different mediums, though many have proposed that the doctrine be reconsidered in light of the ever-increasing world of technology and development.[155]

Since *Katz,* the Court has applied the third-party doctrine to two primary types of cases.[156] First, the Court has held that individuals do not

150. *Id.*

151. *Id.*

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

153. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

154. RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, FOURTH AMENDMENT THIRD-PARTY DOCTRINE (2014).

155. *See, e.g.*, Orin Kerr and Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J. (Aug. 1, 2012), https://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited [https://perma.cc/ZW2Q-RD8G]; Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKLEY TECH L. J. 1239 (2009). *But see, e.g.*, Orin Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561 (2009); Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKLEY TECH L. J. 1199 (2009); Stewart Baker, *Smith v. Maryland as a Good First-Order Estimate of Reasonable Privacy Expectations*, 24 VOLOKH CONSPIRACY (May 4, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/04/smith-v-maryland-as-a-good-first-order-estimate-of-reasonable-privacy-expectations/ [https://perma.cc/DYG7-RNZV].

156. THOMPSON, *supra* note 154, at 1.

have a reasonable expectation that a person with whom they are communicating will not later reveal that information to the police.[157] Second, the Court extended the doctrine to rule that Fourth Amendment protections are not applicable when individuals share information and records with a third-party as a part of a person's business transactions with them.[158] The third-party doctrine does not extend where the third-party is a mere middleman, used to transfer communication between two other individuals.[159]

Smith v. Maryland involved the installation and use of a pen register by law enforcement in order to record telephone numbers from a phone line.[160] The Supreme Court held that the defendant's Fourth Amendment rights were not violated because he did not have an actual expectation of privacy when he dialed phone numbers and that, even if he did, the expectation was not legitimate.[161] Phone numbers are recorded by telephone companies and, thus, there was no privacy interest to be violated.[162]

In a similar vein, the Supreme Court in *United States v. Miller* held that the respondent possessed no Fourth Amendment interest in bank records that were requested by the government in the form of subpoenas.[163] The Court's reasoning clarified the notions put forth in *Smith v. Maryland*. The materials were business records of the banks and not the respondent's private papers.[164] Therefore, there was not a legitimate expectation of privacy since the records were not confidential.[165] The Court held that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party, solidifying the third-party doctrine.[166]

Both *Smith* and *Miller* were decided in the 1970s. Since then, the United States has experienced a mass digital revolution, resulting in individuals sharing their information about every aspect of their lives with various entities.[167] Because of the wave of mass data generation, collection, and processing that has occurred in recent decades, debates have begun about whether lawmakers should take action to protect information in a way that the Fourth Amendment cannot.[168]

The Court's holdings in *Katz, Smith,* and *Mille*r, make Fourth Amendment challenges to forensic genealogy cases particularly fallible.

157. *Id.*
158. *Id.*
159. *Id.*
160. *Smith*, 442 U.S. at 736.
161. *Id.* at 742–43.
162. *Id.*
163. United States v. Miller, 425 U.S. 435, 445 (1976).
164. *Id.* at 440–41.
165. *Id.*
166. *Id.*
167. THOMPSON, *supra* note 154, at 1.
168. *Id.*

Because DNA submissions are voluntarily given to DTCs and other websites like GEDmatch—third parties—the Fourth Amendment does not offer protection to individuals whose genealogical data is accessed by law enforcement. There is no legitimate expectation of privacy when an individual chooses to disclose private information to a third party.

However, Congress can—and has—attempted to extend protection to information through legislation in response to the holdings in cases where the Supreme Court has not under the third-party doctrine. Seven years after the Court's decision in *Smith*, Congress enacted several provisions within the Electronic Communications Privacy Act of 1986 ("ECPA").[169] These provisions require the government to seek a court order before using a pen register or trap and trace device. Under 18 U.S.C. § 3123, a court "shall issue an ex parte order authorizing the installation and use of a pen register or trap and trace device…if the court finds that the attorney for the Government has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[170]

Also included within the ECPA is the Stored Communications Act ("SCA"), through which Congress provided varying degrees of protection to information traditionally outside of the Fourth Amendment's reach under the third-party doctrine.[171] Under 18 U.S.C. § 2703(d), if the government can offer "specific and articulable facts" that records are "relevant and material" to an ongoing criminal investigation, service providers must provide them with "records or other information pertaining to a subscriber."[172] The standard used in this statute has been applied to data such as the to/from address line in an email and the IP addresses of websites a person has visited.[173]

Congress passed other targeted privacy protection laws as well. For example, the Cable Communications Privacy Act of 1984 protects the privacy of cable subscribers.[174] Likewise, the Video Privacy Protection Act protects the privacy of video store customers.[175] Recently, some members of Congress have attempted to limit the reach of the third-party doctrine with respect to transactional data. In response to the Edward Snowden leaks, Senator Rand Paul filed the "Fourth Amendment Restoration Act of

169. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 301, 100 Stat 1868, 1872 (1986).

170. *Id.*

171. 18 U.S.C. § 2703 (2021).

172. *Id.*

173. THOMPSON, *supra* note 154, at 24–25.

174. 47 U.S.C. § 551 (1984). *See also* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) ("A broader look at the legal standards that govern criminal investigations involving new technologies suggests that Congress has often taken the lead, and that judicial decisions interpreting the Fourth Amendment generally have played a secondary role").

175. 18 U.S.C. § 2710 (1988).

2013."[176] The Act is an effort to "stop the National Security Agency from spying on citizens of the United States," and would require the government to obtain a warrant based on probable cause before searching individuals' phone records.[177] Senator Paul also introduced a similar bill called the "Fourth Amendment Preservation and Protection Act of 2013," which would prohibit federal, state, and local governments from accessing information relating to an individual held by a third party in a "system of records."[178]

As Justice Alito stated in *United States v. Jones*, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative" because "a legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[179] Several commentators agree that Congress is best-suited to implement more nuanced and complex policies to address current and foreseeable privacy concerns that supplement our increasingly technological world. As exemplified by the ECPA, SCA, and other acts, Congress is better situated to limit the scope of the third-party doctrine in certain areas through a subject-by-subject approach. As such, forensic genealogy is an area that, because of its increasing role in the United States, should be addressed through legislation.

IV. REGULATORY MEASURES THAT CONGRESS SHOULD ADOPT AND HOW THEY AMELIORATE ETHICAL AND PRIVACY CONCERNS

Congress needs to take immediate action in order to address the problems associated with genealogical information. In doing so, they must balance individual privacy rights with society's interest in an efficient, accurate criminal justice system. I suggest that (A) Congress expand the DOJ's FGGS interim policy into the national policy, as there are many law enforcement agencies that are not currently covered by the regulations set forth by the DOJ. I also suggest Congress do more to protect individual privacy rights by adding more requirements than the interim policy demands. This includes (B) criminalizing DNA theft, (C) prescribing case selection criteria, familial proximity limitations, and methods of maintaining genetic information, and (D) requiring law enforcement to obtain a warrant before receiving access to DNA DTC databases (and GEDMatch). I also recommend that Congress regulate DTCs themselves by (E) requiring an opt-in policy and written informed consent, so that consumers make the affirmative choice to have their genetic information subject to search by the government. Finally, in the alternative, I suggest

176. Fourth Amendment Restoration Act, S. 1121, 113th Cong. (2013).
177. *Id.*
178. Fourth Amendment Preservation and Protection Act, S. 1037, 113th Cong. (2013).
179. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

that (F) Congress implement an accreditation and certification framework for genealogists through an industry standards-based approach. Regardless of the regulatory measures Congress chooses to enforce, it is of utmost importance that law enforcement agencies work with genealogy practitioners to understand the risks and limitations of using forensic genealogy in the context of criminal investigations.

A. Expand the DOJ's Forensic Genealogy Interim Policy into a National Model

As discussed above in Section III, federal legislation currently governing genetic privacy includes only the Health Insurance Portability and Accountability Act of 1966 ("HIPAA") and the Genetic Information Nondiscrimination Act of 2008 ("GINA"). Both are limited in scope and neither apply to DTC DNA testing.[180] About half of the states in the United States have laws protecting genetic privacy, but the patchwork of laws provides no consistency.[181] Thus, a federal regulatory model is necessary to ensure consistency and equal protection of all individuals' genetic privacy.

Certainly, the lack of constitutional protections for information such as DNA data does not prohibit Congress from passing legislation that provides such protections. The field of forensic genealogy and DNA collection is nearly unregulated, aside from the DOJ's interim policy,[182] as discussed in Section III. The DOJ's interim policy offers a reasonable framework in regards to regulating the use of forensic genealogy in the criminal justice system. However, I suggest, along with many professors and legislators alike, that the policy needs to reach further if it is to truly balance society's interest in justice with individual privacy concerns.[183] As discussed above, the DOJ's policy applies only to DOJ agencies and state or local agencies with federal funding to use genetic genealogy searches.[184] However, professors and academics—such as bioethicist Amy McGuire of Baylor College of Medicine—hope and predict that the policy will become a national model. Regulation in this area, ideally, will lead to greater acceptance and trust in this new method of solving crimes.[185]

B. Criminalize DNA Theft

In most American jurisdictions, the nonconsensual collection of human tissue for purposes of DNA analysis is not a crime or a civil

180. Colin McFerrin, *DNA, Genetic Material, and a Look at Property Rights: Why You May Be Your Brother's Keeper*, 19 TEX. WESLEYAN L. REV. 967, 983 (2013).
181. *Id.*
182. *Id.*
183. Kaiser, *supra* note 11.
184. *Id.*
185. *Id.*

violation.[186] Alaska's law is the most comprehensive in this regard, prohibiting "collect[ing] a DNA sample from a person, perform[ing] a DNA analysis on a sample, retain[ing] a DNA sample or the results of a DNA analysis, or disclos[ing] the results of a DNA analysis unless the person first obtained the informed and written consent of the person."[187] The statute also states that DNA samples and resulting DNA analysis are the exclusive property of the person sampled or analyzed.[188]

The nonconsensual collection and analysis of another's DNA is essentially unrestrained by law in the United States.[189] DNA theft should be a separate crime under federal law. Individuals leave genetic material everywhere they go in the form of hair, discarded tissues, used cups, and other items. When third parties retrieve these genetic materials for their own purpose, both the individual's privacy and ability to consent are relinquished, giving rise to ethical issues. While law enforcement is certainly interested in genetic material, other non-governmental parties may also be a concern. For example, concerns have been raised about political parties analyzing opposing candidates, professional sports teams analyzing potential players, and the exploitation of celebrities' genetic information.[190]

A proposed law for DNA theft criminalizes "(1) knowingly taking or storing another person's bodily material (2) without consent (3) for the purpose of analyzing or disclosing the genetic information therein."[191] Proponents of criminalizing DNA theft also emphasize the need for legislation to account for familial relationships and shared genetic information to prevent an individual from having "no recourse against a family member that intentionally or mistakenly shares 'that person's genetic secrets.'"[192] However, the legislation also need not be too stringent, subjecting family members to criminal or civil liability for releasing their own genetic information.[193]

In 2006, the United Kingdom passed a law that criminalized DNA theft.[194] The Human Tissue Act defines the nonconsensual taking of another's bodily material for genetic analysis as a criminal offense, unless it is for an approved purpose. An individual found guilty of violating the act is subject to a fine, three years in prison, or both.[195] Criminalizing DNA theft may seem extraneous to DTC databases and the use of forensic genealogy, but it would serve as another guard against the risk of individuals submitting others' DNA to DTC databases without their

186. Joh, *supra* note 56, at 666.
187. ALASKA STAT. § 18.13.030(a) (2021).
188. ALASKA STAT. § 18.13.010(a).
189. Joh, *supra* note 56, at 666.
190. *Id.* at 666–67.
191. *Id.* at 689.
192. McFerrin, *supra* note 180, at 994.
193. *Id.*
194. Human Tissue Act 2004, c.30 (U.K.).
195. *Id.*

consent. It may also lead to a clearer understanding of Fourth Amendment concerns regarding genetic information, as "the existence of a DNA theft offense expresses a social norm that genetic information, wherever it is found, retains individual privacy interests that deserve protection from theft."[196] The United Kingdom's Human Tissue Act provides an appropriate model for this type of legislation.

C. Congress Should Prescribe Offense Types, Familial Proximity Limits, and the Obligations of Genetic Information Holders

The model for regulating the collection of genetic genealogy should include defined prescriptions in regards to offense types, familial proximity, and obligations to maintain privacy of genetic information. First, the regulatory model should prescribe the offense types, or minimum prescribed penalty, for which forensic genealogy could be applied.[197] The case selection criteria is a preventative measure that has been used in the DOJ's interim policy, as well.[198] Currently, DTC databases have been used primarily to solve violent crimes and cases in which unidentified human remains are found.[199] However, genetic genealogical DNA analysis was used in Colorado to investigate a case involving theft of loose change from a vehicle.[200] Use of forensic genealogy should be limited to violent crimes involving an individual that is a threat to public safety and to cases in which law enforcement is attempting to identify human remains. Additionally, to gain access to DTCs, law enforcement must show that they have exhausted other traditional investigatory measures, as DNA matches from crime scenes are often not dispositive of guilt.[201] Additionally, law enforcement should certify that (1) no matches to suspect profiles were found in NDIS and (2) there is sufficient DNA at the crime scene to yield accurate searches against the databases.[202] Limiting the case selection criteria is supported by public opinion.[203] A study conducted by bioethicists revealed that—in a survey of 1,587 individuals—seventy-nine percent supported the use of forensic genealogy in homicide and rape cases.[204] The same survey yielded

196. Joh, *supra* note 56, at 696.

197. Nathan Scudder et al., *Policy and Regulatory Implications of the New Frontier of Forensic Genomics: Direct-to-Consumer Genetic Data and Genealogy Records*, 31 CURRENT ISSUES IN CRIM. JUST. 194, 208 (2019).

198. U.S. DEP'T OF JUST., *supra* note 117.

199. *See generally* Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 STAN. L. REV. 751 (2011).

200. *Id.* at 781.

201. *Testing DNA: In her new book, Erin Murphy investigates how the criminal justice system misuses genetic identification*, *supra* note 129.

202. Wickenheiser, *supra* note 14, at 121.

203. *Id.* at 120.

204. *Id.*

only thirty-nine percent in support of genealogical DNA analysis in property crime cases.[205]

Second, the regulatory model should prescribe limits on familial proximity in an effort to protect distantly related family members from unnecessary invasions of privacy. The legislation should define how distant a familial relationship can be to be considered as an actionable lead by law enforcement, thereby balancing the cost to distant relatives drawn into a criminal investigation with the benefit of efficiently identifying a suspect.[206]

Lastly, the regulatory model should prescribe the obligations both law enforcement and online DNA databases must adhere to in maintaining privacy of genetic information about crime scenes or unidentified deceased persons.[207] This could include isolating or destroying data collected from DNA databases that did not reveal matches or information from family members that are not involved in the criminal investigation. There is little oversight in these areas aside from the DOJ interim policy and the internal regulations DTCs have created for themselves in regards to maintaining privacy and, as such, a regulatory model should include methods of maintenance to increase consistency. This will also aid in consumers' ability to give informed consent and, likely, will generate public trust.[208]

D. Require Law Enforcement to Obtain a Warrant

A regulatory approach should complement any existing forensic procedures legislation, ensuring that the process used by law enforcement for collecting and using DNA capabilities are seamless.[209] Although its focus is the collection of telecommunications metadata, Australia's Telecommunications (Interception and Access) Act of 1979 provides a good model for this regulatory structure.[210] The Act allows law enforcement to make a request to companies to confirm the existence of records, then requires officers to apply for a writ or search warrant in order to gain access.[211] In the forensic genetic genealogy context, officers would make a request for genetic genealogy providers to confirm the existence of records to a stated level of familial proximity. After confirmation from the company that the records exist, officers should then apply for a search warrant for the records.

Professors and academics in the United States have voiced support of this type of regulation.[212] Natalie Ram of the University of Maryland School of Law, for example, suggests that the police should need a search

205. *Id.*
206. Scudder et al., *supra* note 197, at 198.
207. *Id.* at 202.
208. *Id.* at 208.
209. *Id.*
210. *Id.*
211. *Id.*
212. Kaiser, *supra* note 11.

warrant or other oversight from a magistrate or other judge to conduct a genetic genealogy search.[213] She argues that, in order for law enforcement to gain access to a commercial genetic genealogy provider's records to identify DNA left at a crime scene, the request should be specific, requiring the provider to surrender a only list of users whose genetic data closely matches a genetic profile provided by law enforcement.[214]

These measures would address several concerns. First, they would prohibit law enforcement from obtaining mass information about individuals unrelated to the criminal investigation, preserving individual privacy interests. By requiring law enforcement to state specific and confined familial proximity, many distantly related family members would be safe from having their genetic information accessed by law enforcement. Relatedly, requiring a warrant would demand more precise and diligent investigation on the front end. Thus, law enforcement would be unable to interrupt innocent citizens' lives for the purpose of ruling them out.

E. Require DTCs and Genetic Databases to Include Opt-In Provisions and Demand Written Informed Consent

In an effort to reduce ethical concerns, each DNA DTC provider should be required to have an "opt-in" option through which DNA donors can consent to government searches. Doing so would allow consumers to actively choose whether or not their information could be used for criminal investigation. GEDmatch revised its policy to include an "opt-in" option, whereby consumers could actively agree to be included in searches conducted by government agencies.[215] Consequently, the number of profiles available for police search reduced by around 90%, from roughly 1.4 million to 140,000.[216] This reduction undoubtedly came as a disappointment to many investigators and members of law enforcement, but it is an important step in ensuring that consumers maintain their privacy and provide true informed consent. Amy McGuire, professor of biomedical ethics, projects that, in the long run, federal regulation of this area will make the public more accepting of having its DNA used in police searches. She states, "putting limitations on use of the technology is a really important step towards building public trust."[217]

Recently, FamilyTreeDNA made it possible for consumers to opt-out of familial matching, which prevents their profiles from being subject to searches by the Federal Bureau of Investigation, but simultaneously

213. *Id.*
214. *Id.*
215. *Id.*
216. *Id.*
217. *Id.*

prevents them from finding potential relatives.[218] While the "opt-out" option is certainly a positive step toward increasing informed consent, the "opt-in" method is perhaps the most effective way of ensuring that consumers are actively choosing to subject their genetic information to government searches.

An additional regulatory requirement that some have contemplated is demanding that a written consent form be sent in by genetic donors.[219] A consent form should:

> Inform the donor of the purpose and scope of testing; the length of time the sample and results will be retained; the potential corollary uses, if any, for which the donor's sample and results will be used; and identification of third parties that may conduct any testing or analysis of the sample or results. The form shall also include an "opt-out" provision in which the donor may elect to have the sample and results destroyed upon completion of the stated purpose and scope of testing.[220]

A written consent form does not guarantee that the donor is the actual person who he or she says they are or that the signature is authentic. However, this requirement does provide legitimate deterrence from some of the privacy issues discussed in Section II. It is also yet another active step on the part of the DTC provider to ensure privacy rights are respected and informed consent is given.

F. In the Alternative, Congress Could Implement Industry Standards to Better Regulate the Area of Forensic Genealogy

Another alternative would involve the use of relevant industry standards to regulate the field of forensic genealogy. In other countries, genealogists can receive a certification and agree to abide by a code of ethics. Forensic laboratories have several international accreditation and certification options. Establishing an accreditation framework would likely result in increased community trust in the use of this technology, as practitioners would be required to undergo appropriate training and become acquainted with the risks of using genealogical DNA analysis. Additionally, training processes could be aligned with best practices in forensic analysis, ensuring that both genealogists and members of law enforcement alike

---

218. Salvador Hernandez, *One of the Biggest At-Home DNA Testing Companies is Working with the FBI*, BUZZFEED NEWS (Jan. 31, 2019), https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy [https://perma.cc/LRT4-3ZXU].

219. McFerrin, *supra* note 180, at 996.

220. *Id.*

would be better educated about the advantages and limitations of forensic genealogy in the context of criminal investigations.

Regardless of whether a regulatory or standards-based approach is considered by Congress, however, it is clear that law enforcement agencies need to carefully consider their approach to training and awareness. Many of the issues regarding law enforcement's misuse of DNA information discussed in Section II could be mitigated through an increased awareness by officers, investigators, and judicial officers, who may ultimately need to assess information in the context of a warrant application. The widespread use of DTC services means that family trees generated by genealogists can contain inaccuracies and omissions. Thus, careful consideration by law enforcement agencies should be given to the advantages and disadvantages of this technique. Specifically, agencies should consider the process of obtaining DNA covertly prior to an arrest through discarded items from a suspect and by performing a forensic DNA analysis to compare with the crime scene profile. This method has been used in several cases involving family DNA searching, including the paramount cases of the Grim Sleeper and East Area Rapist.[221] This approach can mitigate risks of drawing innocent individuals into a criminal investigation.

The suggestions I make in this section address several of the issues discussed in Section II. By implementing an opt-in requirement and written informed consent policy, individuals who choose to upload their DNA samples to DTCs and other databases are affirmatively choosing to relinquish some of their genetic privacy interests. Likewise, expanding the DOJ's interim policy into a national model that covers all law enforcement agencies will prevent law enforcement from acquiring and exploiting mass amounts of genetic information, keep the integrity of investigatory procedure intact, and ensure that DNA matches are used only to supplement other evidence when attempting to convict a suspect. By expanding on the interim policy through warrant requirements, more definitive case selection criteria, limiting familial proximity, and outlining the obligations of DTCs and law enforcement in maintaining genetic information, the risk of misuse by law enforcement will be even further mitigated.

However, these suggestions do not address all concerns associated with forensic genealogy. First, this piece focuses primarily on genetic information in the context of criminal investigation. Thus, the risk of genetic information being obtained and exploited by other institutions, such as schools or employers, is not adequately addressed by these legislative suggestions. While it is not currently a pervasive risk, instances of misuse and discrimination by schools using genetic information have taken place, and it would be wise for Congress to consider and address the possibility of it becoming more prevalent if preventative action is not taken. Additionally, my suggestions do not explicitly address racial and ethnic discrimination by

221. *Id.* at 973.

law enforcement through the use of genetic information, an increasing concern as DNA phenotyping becomes more predominant. Requiring a warrant and ensuring that law enforcement performs an adequate investigation before turning to DNA websites does work to mitigate some of the risk of discrimination, but a more comprehensive and holistic plan for addressing discrimination in the context of forensic genealogy should be contemplated by Congress. As the use of this new technology becomes more widespread, it is crucial that consumers, genealogists, law enforcement agencies, and governmental bodies become better educated about the limitations and risks of forensic genealogy. Congress needs to inform itself and legislate this area promptly in order to ensure that many of the risks associated with forensic genealogy are ameliorated and that foreseeable concerns are addressed before they become devastating.

CONCLUSION

Genealogy websites, such as Ancestry.com and 23andMe have given individuals answers about their lineage, their origins, and have—in some cases—reunited families. Additionally, forensic genealogy has revolutionized investigatory practice in the criminal justice field. This technology is a powerful tool, but one that must be appropriately regulated. The privacy risks associated with uploading a DNA sample to a large database are just now beginning to be understood and evaluated. Yet, there are other impending risks that have yet to be seen. As such, Congress should pass legislation soon to combat both the present issues, such as the infringement on individual privacy and misuse by law enforcement, and the foreseeable negative consequences of leaving the field unregulated.