Georgia State University Law Review

Volume 39
Issue 2 *Winter 2023*

Article 14

3-2-2023

A Square Double Helix in a Round Hole: Forensic Genetic Genealogy Searches and the Fourth Amendment

Matthew Sweat
msweat4@student.gsu.edu

A SQUARE DOUBLE HELIX IN A ROUND HOLE: FORENSIC GENETIC GENEALOGY SEARCHES AND THE FOURTH AMENDMENT

Matthew Sweat*

ABSTRACT

A forensic genetic genealogy search (FGGS) involves law enforcement's use of consumer DNA databases to generate leads to solve cold cases. As a result of more modern technological processes, the DNA profiles kept in consumer databases are far more revealing than the DNA profiles stored in the FBI's Combined DNA Index System (CODIS). Accordingly, each DNA profile in a consumer database can be used to identify hundreds of relatives related to the DNA's contributor.

The government's use of consumer DNA databases to locate the perpetrators of horrific, unsolved crimes has generated fans and critics. Supporters of FGGSs argue that, in light of the hundreds of thousands of unsolved crimes, this technique should be used in the name of justice and public safety. Critics of FGGSs argue that the government's access to this kind of information is a Fourth Amendment violation, creating nationwide privacy risks since DNA profiles from only a small portion of the population could enable the government to identify nearly every citizen.

* Assistant Student Writing Editor, *Georgia State University Law Review*; J.D. Candidate, 2023, Georgia State University College of Law. I would like to thank Professor Erin C. Fuse Brown for providing guidance and feedback throughout the writing process and Professor Yaniv Heled for helping me develop the topic for this Note. Additionally, I would like to thank my friends and colleagues on the *Georgia State University Law Review* for their work on this Note and for their selfless efforts to operate this journal. Finally, I would like to thank my wife and our Siberian Husky for all the good memories throughout law school.

This Note analyzes FGGSs in light of current Fourth Amendment jurisprudence. In particular, this Note examines FGGSs under the Katz v. United States framework in light of the uncertainty generated from the landmark Supreme Court decision of Carpenter v. United States. Ultimately, this Note concludes that the Katz framework cannot provide a satisfactory answer for the constitutionality of FGGSs and that state-based positive law fails to provide a workable regulatory framework for FGGSs.

This Note proposes a pragmatic compromise. Similar to the Massachusetts Forensic Science Oversight Board, other states should create interdisciplinary oversight boards to monitor the use of FGGSs at the state level. These boards can implement policy consistent with the 2019 Department of Justice FGGS interim guidelines and update their programs as the federal government develops a more robust regulatory framework to guide the use of this novel and powerful technology.

CONTENTS

INTRODUCTION 608
I. BACKGROUND 612
A. *The Prosecutor's Silver Bullet: DNA* 612
B. *The Fourth Amendment and Genetic Information* 617
II. ANALYSIS 622
A. Maryland v. King *Frames the Debate* 623
B. Carpenter v. United States *and the Fourth Amendment's Application to Modern Technology* 626
C. *Positive Law and FGGSs* 629
III. PROPOSAL 632
A. *Probable Cause and Third-Party DNA Databases* 632
B. *The* Katz *Framework: A Balancing of Competing Interests* 633
1. *The Government Has an Exceptionally Strong Interest in Using FGGSs* 634
2. *DNA Consumers Have an Expectation of Privacy in Their Genetic Information* 636
C. *Positive Law Can Guide the Judiciary* 638
1. *The Limitations of a State-Based Solution* 638
2. *The Unlikely Prospect of a Comprehensive Federal Solution* 640
3. *The Middle Path* 641
CONCLUSION 642

INTRODUCTION

A young couple visiting Seattle from British Columbia were brutally murdered in the fall of 1987.[1] Law enforcement collected DNA from the crime scene but were unable to identify suspects for more than thirty years.[2] In 2018, investigators shared the source DNA from the crime scene with Parabon NanoLabs (Parabon), a DNA technology company in Virginia, in search of a breakthrough.[3] Parabon used the DNA in two ways: It generated a description of what the killer might look like, and it uploaded the DNA profile to GEDmatch, a "DNA comparison and analysis website" that aggregates DNA profiles created by direct-to-consumer DNA testing companies.[4] Cece Moore, the self-taught "citizen scientist" who has become Parabon's chief genetic genealogist, used two second-cousin matches from GEDmatch to build a family tree that indicated William Earl Talbott II was the source of the DNA left at the Seattle crime scene.[5] Armed with a

1. Peter Aldhous, *A Double Murder from 1987 Was Just Solved Thanks to the Genealogy Website Used for the Golden State Killer*, BUZZFEED NEWS (May 18, 2018, 3:29 PM), https://www.buzzfeednews.com/article/peteraldhous/cook-van-cuylenborg-murder-DNA-genealogy [https://perma.cc/ZYH9-5C5N].

2. *See SeaTac Man Convicted of 1987 Murders of Canadian Couple After DNA Evidence Linked Him to Case*, SEATTLE TIMES [hereinafter SEATTLE TIMES], https://www.seattletimes.com/seattle-news/crime/seatac-man-convicted-of-1987-murders-of-canadian-couple-after-dna-evidence-linked-him-to-case/ [https://perma.cc/XYN7-4C6Q] (June 28, 2019, 3:58 PM); Megan Molteni, *The First Murder Case to Use Family Tree Forensics Goes to Trial*, WIRED (June 10, 2019, 12:43 PM), https://www.wired.com/story/the-first-murder-case-to-use-family-tree-forensics-goes-to-trial/ [https://perma.cc/4A78-VZL7].

3. SEATTLE TIMES, *supra* note 2; *About Parabon NanoLabs: Innovative DNA Technologists*, PARABON NANOLABS [hereinafter *About Parabon NanoLabs*], https://parabon-nanolabs.com/about.html [https://perma.cc/WU3E-C9BQ] (noting that "the company is most widely known for revolutionizing the field of DNA forensics").

4. *About GEDmatch*, GEDMATCH, https://www.gedmatch.com/about-us [https://perma.cc/KFN8-8UC3]; SEATTLE TIMES, *supra* note 2.

5. Antonio Regalado & Brian Alexander, *The Citizen Scientist Who Finds Killers from Her Couch*, MIT TECH. REV. (June 22, 2018), https://www.technologyreview.com/2018/06/22/142148/the-citizen-scientist-who-finds-killers-from-her-couch/ [https://perma.cc/JEC2-WMH4]; SEATTLE TIMES, *supra* note 2 ("[Moore] identified second cousins in the GEDmatch databank and from there, developed two family trees, one going back to the suspect's paternal grandmother and the other to his maternal great-grandparents . . . Talbott—who was 24 at the time of the murders—is the only male carrier for the mix of DNA from the two families . . . ."); *About Parabon NanoLabs*, *supra* note 3.

laptop, a notebook, and a whiteboard, Moore did in two hours what Snohomish County investigators failed to do for decades.[6]

Acting on this lead, detectives surveilled Talbott.[7] When he inadvertently dropped a used paper coffee cup from his truck, law enforcement confirmed that DNA from the cup matched the source DNA from the Seattle crime scene that had been given to Parabon.[8] As a result, Talbott, who did not share his DNA with GEDmatch, became the first defendant tried and convicted by a jury based on a lead generated by a forensic genetic genealogy search (FGGS).[9] Criminal investigators are increasingly turning to FGGSs to generate leads for cold cases; in fact, FGGSs generated twenty-eight cold case suspects in 2018 alone.[10] However, not everyone is thrilled about this emerging law enforcement "gold mine" as concerns proliferate regarding privacy and unchecked policing power.[11] Legal commentators are divided over whether law enforcement's use of commercial DNA

6. *The Genetic Detective: The Case of the Missing Lovebirds* (ABC television broadcast May 26, 2020), https://abc.com/shows/the-genetic-detective/episode-guide/season-01/01-the-case-of-the-missing-lovebirds [https://perma.cc/4JN4-N5DP] (40 min., 50 sec.); Regalado & Alexander, *supra* note 5.

7. SEATTLE TIMES, *supra* note 2.

8. *Id.*

9. Caleb Hutton, *Life in Prison for 1987 Killer of Young Canadian Couple*, SEATTLE WKLY. (July 24, 2019, 11:11 AM), https://www.seattleweekly.com/news/life-in-prison-for-1987-killer-of-young-canadian-couple/ [https://perma.cc/9UWV-2B85]; Megan Molteni, *Man Found Guilty in a Murder Mystery Cracked by Cousins' DNA*, WIRED (June 28, 2019, 3:05 PM), https://www.wired.com/story/man-found-guilty-in-a-murder-mystery-cracked-by-cousins-dna/ [https://perma.cc/ANR6-CDMY]; *see* U.S. DEP'T OF JUST., INTERIM POLICY: FORENSIC GENETIC GENEALOGICAL DNA ANALYSIS AND SEARCHING 3 (2019), https://www.justice.gov/olp/page/file/1204386/download [https://perma.cc/68QG-WW9S] ("Forensic genealogy is law enforcement's use of DNA analysis combined with traditional genealogy research to generate investigative leads for unsolved violent crimes.").

10. Robert Gearty, *DNA, Genetic Genealogy Made 2018 the Year of the Cold Case: 'Biggest Crime-Fighting Breakthrough in Decades,'* FOX NEWS (Dec. 19, 2018, 6:45 AM), https://www.foxnews.com/us/dna-genetic-genealogy-made-2018-the-year-old-the-cold-case-biggest-crime-fighting-breakthrough-in-decades [https://perma.cc/PZ6R-UEXP]; *see* Jacob Stern & Sarah Zhang, *The Victims Left Behind by Genetic Genealogy*, ATLANTIC (Jan. 27, 2021), https://www.theatlantic.com/science/archive/2021/01/genetic-genealogy-race/616171/ [https://perma.cc/BQU5-7F8M] (analyzing the racial makeup of the "104 murder victims whose alleged killers had been identified" using FGGSs across twenty-seven states from April 2018 to April 2020).

11. 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, 5:00 AM), https://www.latimes.com/california/story/2019-11-24/law-enforcement-dna-crime-cases-privacy?utm_source=The+Appeal&utm_campaign=6227545180 [https://perma.cc/3FL2-AHES] (discussing the "growing concerns that the race to use genealogical databases will have serious consequences, from its inherent invasion of privacy to the implications of broadened police power").

profiles in third-party (private or open-source) databases to generate investigatory leads violates the Fourth Amendment's protection against unreasonable search and seizure.[12]

A Fourth Amendment search is valid when conducted within the scope of a warrant issued on the basis of probable cause.[13] The Supreme Court considers searches lacking judicial sanction, "without prior approval by judge or magistrate, per se unreasonable" and in violation of the Fourth Amendment.[14] The Court, however, has also recognized that absent a warrant, Fourth Amendment protections can vary depending on the overall reasonableness of the search.[15] Such reasonableness is determined by balancing the government's interest against the individual's expectation of privacy in that activity.[16] Some commentators consider law enforcement's warrantless use of

12. The Fourth Amendment provides:

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

U.S. CONST. amend. IV. *See* Jamie M. Zeevi, Note, *DNA Is Different: An Exploration of the Current Inadequacies of Genetic Privacy Protection in Recreational DNA Databases*, 93 ST. JOHN'S L. REV. 767, 808 (2019) ("It remains to be seen whether the Supreme Court will deem DNA a unique type of data and whether it will find [forensic genetic genealogy searching] subject to Fourth Amendment protections"). *Compare* Amelia Putnam, *A Genetic Panopticon of Our Own Making: How the Fourth Amendment Applies to Commercial Genealogy DNA Testing*, 56 CRIM. L. BULL. 221 (arguing that using commercial genealogical databases to aid in criminal investigations is a search per the Fourth Amendment due to privacy and property interests that people have in their DNA), *with* Genevieve Carter, *The Genetic Panopticon: Genetic Genealogy Searches and the Fourth Amendment*, 18 NW. J. TECH. & INTELL. PROP. 311, 334 (2021) (calling for a legislative solution because "[s]haring genetic information for the express purpose of being found by family members in public DNA databases forecloses the possibility of Fourth Amendment protections under [the relevant doctrine]").

13. U.S. CONST. amend. IV.

14. Katz v. United States, 389 U.S. 347, 357 (1967).

15. *See* Maryland v. King, 569 U.S. 435, 436, 448 (2013); Winston v. Lee, 470 U.S. 753, 767 (1985) ("[T]he Fourth Amendment's command that searches be reasonable requires that when the State seeks to intrude [without a warrant] upon an area in which our society recognizes a significantly heightened privacy interest, a more substantial justification is required to make the search reasonable." (internal quotation marks omitted)); *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (noting that Fourth Amendment protections are extended when "first[,] . . . a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, . . . the expectation [is] one that society is prepared to recognize as reasonable" (internal quotation marks omitted)).

16. *King*, 569 U.S. at 448 (noting that determining reasonableness "requires a court to weigh 'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy." (alteration in original) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))).

commercial DNA housed in third-party databases an unreasonable search in violation of the Fourth Amendment.[17] Conversely, others argue that warrantless use of FGGSs does not amount to an unreasonable search because of the government's considerable interest in solving crime.[18] Finally, other commentators conclude that current Fourth Amendment jurisprudence cannot accommodate FGGSs, necessitating legislation or updated Supreme Court doctrine.[19]

This Note argues that the Fourth Amendment and the traditional warrant system are ill-equipped to accommodate commercial DNA stored in private databases. Furthermore, states are ill-equipped to regulate the use of this information due to the shared nature of genetic information[20] and the ubiquity and ease of access of online databases. Considering these realities, this Note contributes to the growing literature by proposing that states who wish to use this technology in criminal investigations pass legislation to establish civilian forensic science oversight boards that can monitor law enforcement's use of FGGSs pursuant to the 2019 Department of Justice (DOJ) interim guidelines.[21] Part I familiarizes the reader with the evolution of forensic DNA and the existing legal frameworks that could bear on this technology, including case law, state statutes, and the 2019 DOJ interim guidelines for FGGSs. Part II analyzes Fourth Amendment jurisprudence relating to DNA and other emerging technologies and

17. Putnam, *supra* note 12; Drew M. Baldwin, Note, *Redefining the Third-Party Doctrine:* Carpenter*'s Effect on DNA Privacy*, 108 KY. L.J. 153, 162 (2020) ("DNA data stored in third-party databases should be given the same protection [as the information in *Carpenter v. United States*] under the Fourth Amendment and should remain private."); Jennifer Lynch, *Forensic Genetic Genealogy Searches: What Defense Attorneys Need to Know*, CHAMPION, Nov. 2020, at 22, 28 (arguing that law enforcement's use of FGGSs "should never be allowed — even with a warrant").

18. Shanni Davidowitz, Note, *23andEveryone: Privacy Concerns with Law Enforcement's Use of Genealogy Databases to Implicate Relatives in Criminal Investigations*, 85 BROOK. L. REV. 185, 215 (2019).

19. *E.g.*, Michael I. Selvin, Note, *A Too Permeating Police Surveillance: Consumer Genetic Genealogy and the Fourth Amendment After* Carpenter, 53 LOY. L.A. L. REV. 1015, 1069 (2020); Rebecca Gold, Comment, *From Swabs to Handcuffs: How Commercial DNA Services Can Expose You to Criminal Charges*, 55 CAL. W.L. REV. 491, 518 (2019).

20. *See* Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 903 (2015) (discussing how, in contrast with the standard traits of personal property, people "cannot simply sell or otherwise alienate [their] interest in [their] genetic information" because relatives share their DNA with their biological relatives).

21. *See generally* U.S. DEP'T OF JUST., *supra* note 9 (describing the DOJ's policy on FGGSs).

considers how the Court might analyze FGGSs. Part III examines the problem with a state-based regulatory approach and proposes that state civilian forensic science oversight boards present the best path forward until a federal regulatory scheme for the forensic use of commercial DNA is established.

I. BACKGROUND

The Supreme Court has said that "DNA testing has an unparalleled ability both to exonerate the wrongly convicted and to identify the guilty."[22] This Section will explain the history of this technology, how DNA is treated in constitutional law, and recent attempts to regulate the use of FGGSs in criminal investigations.

A. The Prosecutor's Silver Bullet: DNA

In 1984, Alec Jeffreys produced the first "DNA fingerprint"—a sequence of bars on photographic film corresponding to an individual's unique DNA that revealed kinships when compared against other DNA fingerprints.[23] In 1987, Jeffreys developed the first DNA profile—a unit of information which "require[s] smaller forensic samples" than a DNA fingerprint and can be turned into a personal identifier in the form of "a sequence of numbers."[24] This breakthrough enabled DNA databases to be created.[25] Considered the "pinnacle" of forensic evidence, DNA analysis quickly proved capable of both

22. Dist. Att'y's Off. for the Third Jud. Dist. v. Osborne, 557 U.S. 52, 55 (2009).

23. Robin McKie, *Eureka Moment that Led to the Discovery of DNA Fingerprinting*, GUARDIAN (May 23, 2009, 7:01 PM), https://www.theguardian.com/science/2009/may/24/dna-fingerprinting-alec-jeffreys [https://perma.cc/2EG6-P9MG]. After realizing the significance of his discovery, Jeffreys and his staff soon realized this technique might be able to identify individuals from crime scene evidence. *Id.* To test his theory, he cut himself and left blood marks around the lab. *Id.* When those samples revealed the intact DNA, Jeffreys's laboratory "became the first setting for a DNA crime scene analysis." *Id.*

24. *Id.* ("[DNA profiles] use pieces of DNA from only a few selected sites on a person's chromosomes. Repetitions of DNA at these sites are counted, producing a set of numbers that act as a person's DNA identifier.").

25. *Id.*

solving crimes and exonerating the wrongly accused.[26] In 1994, the FBI launched the Combined DNA Index System (CODIS), a system that has "revolutionized criminal investigation" by serving as a central database through which police can compare DNA evidence from local crime scenes to all other DNA profiles in the system.[27] CODIS matches DNA from a crime scene with DNA already in the database by examining short tandem repeats (STRs), which "are areas of a person's DNA that are repeated" and are unique to each person.[28] When the database reveals at least a partial STR match, law enforcement can deduce that they have found a biological relative of the criminal suspect.[29]

Using a partial STR match to generate investigative leads from the DNA of a suspected criminal's relative constitutes a familial DNA search.[30] British officials conducted the first familial DNA search to solve a decades-long cold case in 2002, when a partial STR match led investigators to the DNA profile of the son of the perpetrator of

26. Erin Murphy, *The Art in the Science of DNA: A Layperson's Guide to the Subjectivity Inherent in Forensic DNA Typing*, 58 EMORY L.J. 489, 490, 512 (2008); *How DNA Analysis Has Revolutionized Criminal Justice*, DEAKIN UNIV.: THIS., https://this.deakin.edu.au/career/how-dna-analysis-has-revolutionised-criminal-justice [https://perma.cc/SD85-UECU]; *DNA Exonerations in the United States*, INNOCENCE PROJECT, https://innocenceproject.org/dna-exonerations-in-the-united-states/ [https://perma.cc/WH52-NHJL].

27. Victoria Romine, Comment, *Crime, DNA, and Family: Protecting Genetic Privacy in the World of 23andMe*, 53 ARIZ. ST. L.J. 367, 375–76 (2021); *see Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet [https://perma.cc/4F8G-B3KD]; *see also* Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1375 (2019); Carter, *supra* note 12, at 313–14.

28. Romine, *supra* note 27, at 376.

29. Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 300 (2010) (describing a process known as "intentional familial searching"); Romine, *supra* note 27, at 377 ("If a person shares STRs with someone else, there is a likelihood that the two individuals are related.").

30. Murphy, *supra* note 29, at 297; HON. NANCY GERTNER, LISA KAVANAUGH, ADRIENNE LYNCH & ANN MARIE MIRES, FORENSIC SCI. OVERSIGHT BD., REPORT ON S.2480, "AN ACT PERMITTING FAMILIAL SEARCHING AND PARTIAL DNA MATCHES IN INVESTIGATING CERTAIN UNSOLVED CRIMES" AND RELATED RECOMMENDATIONS PERTAINING TO G.L. C.22E GOVERNING THE MASSACHUSETTS STATEWIDE DNA DATABASE 4 (2021), https://www.mass.gov/doc/forensic-science-oversight-board-familial-dna-searching-report-march-24-2021/download [https://perma.cc/SKZ3-FKN9]; *see* James Rainey, *Familial DNA Puts Elusive Killers Behind Bars. But Only 12 States Use It.*, https://www.nbcnews.com/news/us-news/familial-dna-puts-elusive-killers-behind-bars-only-12-states-n869711 [https://perma.cc/E8X7-FU2N] (Apr. 28, 2018, 6:00 AM) (providing a real-life example of familial searching).

multiple rapes.[31] California became the first state to implement familial DNA searching in 2008, but not all American jurisdictions have followed suit.[32] Of the states that permit familial DNA searching, "nearly all impose limits on when it can be used: most frequently in cases involving public safety risks, violent crimes, or after the exhaustion of all other investigatory leads."[33] A landmark moment for familial DNA searches occurred in 2010 when Christopher Franklin, whose DNA had recently been added to a California government database because of a weapons charge, inadvertently led investigators to his father, the "Grim Sleeper," a man accused of murdering at least ten young women in Los Angeles.[34] Acting on the lead from Franklin's DNA, investigators surveilled Franklin's father, Lonnie Franklin Jr., until DNA testing from "a discarded piece of pizza" revealed Lonnie to be the murderer and rapist who had evaded law enforcement for decades.[35]

FGGSs are a recent phenomenon made possible by the exponential growth in direct-to-consumer commercial DNA testing.[36] Although the underlying concept is the same, the technique used in the direct-to-consumer DNA analysis differs from traditional familial DNA searches in that it relies on different DNA analysis technology and it

31. Murphy, *supra* note 29, at 301.

32. Romine, *supra* note 27, at 377 (noting that "critics [are] concerned with Fourth Amendment issues and the impact on racial minorities"); Rainey, *supra* note 30 (noting that, as of 2018, "just 12 states . . . employ familial DNA in criminal cases").

33. Romine, *supra* note 27, at 378. For an examination of requirements to request familial DNA testing in various states, see generally MICHAEL B. FIELD, SANIYA SEERA, CHRISTINA NGUYEN & SARA DEBUS-SHERRILL, STUDY OF FAMILIAL DNA SEARCHING POLICIES AND PRACTICES: CASE STUDY BRIEF SERIES (2017), https://www.ojp.gov/pdffiles1/nij/grants/251081.pdf [https://perma.cc/VJ36-FQVU].

34. Greg Miller, *Scientists Explain How Familial DNA Testing Nabbed Alleged Serial Killer*, SCI. (July 12, 2010), https://www.science.org/news/2010/07/scientists-explain-how-familial-dna-testing-nabbed-alleged-serial-killer [https://perma.cc/4WTD-PJXE]; Kelly Lowenberg, *Familial DNA Searching and Abandoned DNA Identify the Grim Sleeper Serial Killer*, STAN. L. SCH.: L. & BIOSCIENCES BLOG (July 8, 2010), https://law.stanford.edu/2010/07/08/familial-dna-searching-and-abandoned-dna-identify-the-grim-sleeper-serial-killer/ [https://perma.cc/5HFK-HH2F].

35. *See* sources cited *supra* note 34.

36. Heather Murphy, *Sooner or Later Your Cousin's DNA Is Going to Solve a Murder*, N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/us/golden-state-killer-dna.html [https://perma.cc/2ZN4-3HSG] (explaining it is probable that any American's name can be derived from a partial match in a third-party database "even if you have never taken a DNA test" since "[w]e all have at least 800 [third cousins] out there somewhere, and there's a good chance that some were once excited enough about genealogy to join GEDMatch or FamilyTreeDNA").

uses third-party, not government, databases.[37] Consumers generally use these DNA tests to learn about their own medical predispositions or genealogical information.[38] The popularity of direct-to-consumer DNA tests has exponentially increased: "By the start of 2019, more than 26 million consumers had added their DNA to four leading commercial ancestry and health databases."[39] This exponential growth is seen in DNA databases that are outside CODIS.[40] Indeed, "privately held companies [like Ancestry and 23andMe] now have some of the world's largest collections of human DNA."[41] Unlike the STR DNA profiles in CODIS that reveal only partial or complete matches, direct-to-consumer DNA tests analyze single nucleotide polymorphisms (SNPs), or the "'coding' regions of the consumer's" DNA.[42] Because SNPs are responsible for the genetic differences among people, they can reveal deeply personal information, including phenotypic traits and predisposition for specific diseases.[43] Since CODIS does not analyze SNP DNA profiles, law enforcement must use "vendor laboratories" (like Parabon) to create the SNP profiles from crime scene DNA and then upload these profiles to a third-party database.[44]

GEDmatch, "a publicly searchable database that allows users who have had their DNA analyzed elsewhere to more deeply investigate their ancestry," is a popular platform for direct-to-consumer DNA testers who want to learn more about their ancestry.[45] GEDmatch analyzes SNPs among uploaded DNA profiles, "looking for long

37. U.S. DEP'T OF JUST., *supra* note 9 , at 2–3 (comparing FGGS analysis to STR DNA typing).

38. *See What Is Direct-to-Consumer Genetic Testing?*, NAT'L LIBR. MEDICINE: MEDLINEPLUS, https://medlineplus.gov/genetics/understanding/dtcgenetictesting/directtoconsumer/ [https://perma.cc/5VXG-UXYU] (June 21, 2022).

39. Antonio Regalado, *More than 26 Million People Have Taken an At-Home Ancestry Test*, MIT TECH. REV. (Feb. 11, 2019), https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/ [https://perma.cc/MY9P-2KRA].

40. Carter, *supra* note 12, at 312, 315 ("[An FGGS] is an investigative tool that is entirely separate from the FBI CODIS system.").

41. Regalado, *supra* note 39.

42. Claire Abrahamson, Note, *Guilt by Genetic Association: The Fourth Amendment and the Search of Private Genetic Databases by Law Enforcement*, 87 FORDHAM L. REV. 2539, 2547, 2549 (2019).

43. *Id.* at 2549; Romine, *supra* note 27, at 379.

44. *See* U.S. DEP'T OF JUST., *supra* note 9.

45. Selvin, *supra* note 19, at 1020; Carter, *supra* note 12, at 320.

stretches that match, thus indicating familial ties."[46] As of November 2020, GEDmatch had 1.45 million users.[47] Since GEDmatch can consistently identify relatives as remote as third cousins, research indicates that their current base of user DNA can identify 60% of white Americans.[48] This extraordinary number is a result of experts' estimations that the average American has between 200 and 800 third cousins.[49] In the wake of privacy concerns following Utah law enforcement's use of an FGGS to identify the perpetrator of a "lesser crime," instead of a "violent crime" per GEDmatch's terms of service, GEDmatch changed its official policy.[50] Under the new policy, users are excluded from law enforcement searches unless they affirmatively opt in.[51] Approximately 14% of GEDmatch users have opted in.[52] Consumer preference was ignored in 2019, however, when a Florida judge granted a warrant allowing an Orlando detective, working with Parabon, to search GEDmatch's full database, including the 86% of profiles who had not opted in to share their DNA with law enforcement.[53] With an ever-increasing amount of genetic information available in third-party databases, the law needs to define an

46. Selvin, *supra* note 19, at 1020.

47. Lynch, *supra* note 17, at 23.

48. *Id.*; Jocelyn Kaiser, *We Will Find You: DNA Search Used to Nab Golden State Killer Can Home in on About 60% of White Americans*, SCI. (Oct. 11, 2018), https://www.science.org/content/article/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white [https://perma.cc/U75S-N3PQ].

49. Romine, *supra* note 27, at 373 (estimating that every American has "nearly 200 third cousins" (quoting Nsikan Akpan, *Genetic Genealogy Can Help Solve Cold Cases. It Can Also Accuse the Wrong Person.*, PBS NEWSHOUR (Nov. 7, 2019, 5:15 PM), https://www.pbs.org/newshour/science/genetic-genealogy-can-help-solve-cold-cases-it-can-also-accuse-the-wrong-person [https://perma.cc/6SUK-BCMF])); Jesse Schwab, *New DOJ Policy Gives Genealogy Website Users Weak Privacy Protections from Law Enforcement*, HARV. C.R.-C.L. L. REV.: AMICUS BLOG (Oct. 3, 2019), https://harvardcrcl.org/new-doj-policy-gives-genealogy-website-users-weak-privacy-protections-from-law-enforcement/ [https://perma.cc/VDJ7-KNZH] (estimating that "[m]ost people have around 800" third cousins).

50. Selvin, *supra* note 19, at 1023–24.

51. *Id.*

52. *Id.* (noting that "only 185,000 of GEDmatch's 1.3 million users have chosen to opt-in"); Lynch, *supra* note 17, at 24 (noting that about 15% of GEDmatch users opted in after the policy changed).

53. *See* Kashmir Hill & Heather Murphy, *Your DNA Profile Is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES, https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html#:~:text=Profile%20is%20Private%3F-,A%20Florida%20Judge%20Just%20Said%20Otherwise,enforcement%20agencies%20across%20the%20country [https://perma.cc/9MXW-RRUJ] (Dec. 30, 2019).

investigator's right to this information to protect individual privacy rights.

B. The Fourth Amendment and Genetic Information

The Fourth Amendment protects citizens' privacy from unreasonable intrusion from law enforcement.[54] Absent consent, law enforcement must first obtain a warrant that is based on "probable cause" to search persons or their property.[55] This Amendment was a reaction to "writs of assistance," or general warrants, that granted eighteenth-century British revenue officers the authority to search ships for smuggled goods at their discretion.[56] Indeed, John Adams considered the negative reaction to these writs to be the seed of independence.[57] The Supreme Court considers "an objective predetermination of probable cause" by a neutral magistrate to be a safeguard against the type of unchecked police discretion that violates the Fourth Amendment.[58]

The Fourth Amendment has since evolved to accommodate new technologies and a changing society.[59] In 1967, the Supreme Court modernized Fourth Amendment jurisprudence in *Katz v. United States* by rejecting a nineteenth-century property-based interpretation of the Fourth Amendment in considering whether constitutional protections

54. *See* U.S. CONST. amend. IV.

55. *See id.*; Alexis B. Hill, Note, *I Just Took a DNA Test, Turns Out My Relative's a Murder Suspect: Restoring Fourth Amendment Balance to Direct-to-Consumer DNA Testing Companies*, 89 GEO. WASH. L. REV. 1046, 1064 (2021). Note that consent can come either directly from the individual or through a third-party. Hill, *supra*.

56. Boyd v. United States, 116 U.S. 616, 624–25 (1886).

57. *Id.* at 625 (quoting Adams as characterizing resistance to these writs as "the first act of opposition to the arbitrary claims of Great Britain" and the origin of "the child Independence" in the colonies).

58. Katz v. United States, 389 U.S. 347, 357, 358 (1967) (quoting Beck v. State of Ohio, 379 U.S. 89, 96 (1964)).

59. *Compare Boyd*, 116 U.S. at 617–18 (discussing whether the seizure of thirty-five cases of plate glass violated the Fourth Amendment), *with Katz*, 389 U.S. at 360–62 (Harlan, J., concurring) (shifting away from a property analysis in favor of a "reasonable expectations" analysis when considering whether the government's wiretapping of a public phone booth was a search within the Fourth Amendment), *and* United States v. Miller, 425 U.S. 435, 444–45 (1976) (creating the third-party doctrine as an exception to the warrant requirement in holding that an individual lost his reasonable expectation of privacy in bank records when he voluntarily provided such information to the bank).

extended to telephone calls and guarded against "the uninvited ear."[60] Concurring with the holding that the government could not wiretap a phone booth to record a citizen's conversation pertaining to illegal gambling, Justice Harlan established a new standard to protect against warrantless searches.[61] Justice Harlan's test requires that the citizen have an actual, "reasonable expectation of privacy" in the matter at hand and that society recognizes, or is "prepared to recognize," the citizen's expectation as reasonable.[62] Thus, Justice Harlan's test expanded protections beyond just a protection in personal property such that the reasonableness of the warrantless search or seizure will subsequently turn on the reasonableness of the individual's expectation of privacy.[63]

Introduced in *United States v. Miller*, the third-party doctrine clarified the reasonable expectation analysis outlined in *Katz*.[64] In *Miller*, the Court refused to extend Fourth Amendment protection to a plaintiff's bank records when the plaintiff voluntarily gave the bank the information in question.[65] Legally, the defendant could not object to the government's access to this information.[66] Under the original articulation of the third-party doctrine, a citizen who voluntarily submitted DNA to a commercial or open-source database would have no reasonable expectation of privacy in that information, and law enforcement's access to that information would not constitute a Fourth Amendment search.[67] In 2018, however, the Supreme Court declined

60. *See Katz*, 389 U.S. at 352, 353 ("[T]he premise that property interests control the right of the [g]overnment to search and seize has been discredited." (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)).

61. *See id.* at 361 (Harlan, J., concurring); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2237 (2018) (Thomas, J., dissenting).

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

63. *See id.*; Abrahamson, *supra* note 42, at 2555.

64. Carter, *supra* note 12, at 326 ("Specifically, the [C]ourt held that an individual loses a reasonable expectation of privacy under the Fourth Amendment when the individual volunteers information to a third party."); United States v. Miller, 425 U.S. 435, 442–43 (1976).

65. *Miller*, 425 U.S. at 442 (affirming the proposition set forth in *Katz* that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection" (quoting *Katz*, 389 U.S. at 351) (alteration in original)). The Court reaffirmed this holding in *Smith v. Maryland* three years later. Smith v. Maryland, 442 U.S. 735 (1979).

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

67. Selvin, *supra* note 19, at 1041.

to extend the third-party doctrine to the "novel circumstances" presented in *Carpenter v. United States*,[68] which raises legitimate questions about the doctrine's applicability to information that is inherently revealing.

Considering the government's warrantless access of cell phone data an unreasonable search under the Fourth Amendment, the Court in *Carpenter* distinguished cell site location information (CLSI) from other types of information covered by the third-party doctrine.[69] In noting that CLSI is constantly being accumulated by wireless carriers "for their own business purposes" and that individuals carry their cell phones everywhere, the Court determined that this information "provides an all-encompassing record of the holder's whereabouts."[70] Accordingly, the Court concluded that cell phone owners retain an expectation of privacy in their physical movements, so CLSI could not be accessed without a warrant.[71]

In dissent, Justice Gorsuch lamented the Court's return to the judicially centered approach of the *Katz* framework.[72] Concerned with the ambiguity inherent in the *Katz* "reasonable expectation of privacy test," Justice Gorsuch's dissent advocated for judges to look "to positive law rather than intuition for guidance on social norms."[73] Of note, each of the four *Carpenter* dissents expressed, in varying degrees, preference for a property-based conception of the Fourth Amendment over the *Katz* balancing framework.[74] Commentators are

68. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217. The "novel circumstances" were the "the unique nature of cell phone location records" and its ability to record an individual's movement. *Id.*

69. *Carpenter*, 138 S. Ct. at 2214, 2216–17.

70. *Id.* at 2212, 2217.

71. *Id.* at 2217.

72. *See id.* at 2265–66 (Gorsuch, J., dissenting) (rejecting the idea that judges rather than legislators should determine whether society recognizes a legitimate expectation of privacy).

73. *Id.* at 2265 (internal quotations omitted). For an exploration of the positive law model in Fourth American jurisprudence, see William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1831 (2016).

74. *Carpenter*, 138 S. Ct. at 2223, 2224 (Kennedy, J., dissenting) (believing the majority's "stark departure from relevant Fourth Amendment precedents . . . is . . . unnecessary and incorrect" and that the Court unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded

currently divided over what *Carpenter*'s holding means for genetic genealogy searches.[75]

In *Maryland v. King*, the Supreme Court analogized the use of a DNA test on an arrestee to other policing identification procedures and refused to extend Fourth Amendment protections to law enforcement's warrantless use of the DNA test.[76] In *King*, Maryland police swabbed DNA from the inside of the cheek of a man arrested for assault "[a]s part of a routine booking procedure."[77] Using CODIS, Maryland police linked this DNA sample to an unsolved rape for which the arrested man was subsequently tried and convicted.[78] After weighing the arrestee's diminished expectation of privacy against the strong government interest in obtaining the DNA, the Court held that the warrantless buccal swab did not violate the Fourth Amendment.[79] The Court considered the use of DNA to be the successor of photography and fingerprinting—technologies law enforcement freely use to identify suspects in custody.[80]

In dissent, Justice Scalia, joined by Justices Ginsburg, Sotomayor, and Kagan, lambasted the majority's use of the term "identify" to

---

the analytic framework that pertains in these cases."); *id.* at 2239 (Thomas, J., dissenting) (lamenting the *Katz* test's focus on "privacy" and asserting that the Fourth Amendment protections were traditionally "understood largely in terms of property rights"); *id.* at 2260 (Alito, J., dissenting) ("Carpenter indisputably lacks any meaningful property-based connection to the cell-site records owned by his provider. Because the records are not Carpenter's in any sense, Carpenter may not seek to use the Fourth Amendment to exclude them."); *id.* at 2268–69 (Gorsuch, J., dissenting) (arguing that "ancient principles" of property law, such as a bailment, "may help [the Court] address modern data cases too").

75. *See, e.g.*, Putnam, *supra* note 12 (noting that the Court's decision in *Carpenter* "may signal the Court's eventual willingness to reconsider whether the Third Party Doctrine truly has a place under the Fourth Amendment"); Baldwin, *supra* note 17 ("If the Supreme Court considers cell phone location data to be a form of data that is qualitatively different from business records, then DNA data must be considered qualitatively different, too." (internal quotation marks omitted)); Jasper Ford-Monroe, Note, *Why Familial Searches of Civilian DNA Databases Can and Should Survive* Carpenter, 72 HASTINGS L.J. 1717, 1730–32 (2021) ("Strictly speaking, *Carpenter* has no effect on FGGS[s] one way or another because *Carpenter* was a narrow holding about cell site data, and DNA is not cell site data." (footnote omitted)).

76. *See* Maryland v. King, 569 U.S. 435, 461, 465 (2013).

77. *Id.* at 440.

78. *Id.* at 440, 444–45.

79. *Id.* at 447, 465.

80. *Id.* at 461 ("DNA identification of arrestees . . . is 'no more than an extension of methods of identification long used in dealing with persons under arrest.'" (quoting United States v. Kelly, 55 F.2d 67, 69 (2d Cir. 1932))).

describe using DNA matching technology to solve a cold case.[81] According to the dissent, the Fourth Amendment bars searches in criminal investigations that are not based on individualized suspicion and are done to detect "ordinary criminal wrongdoing."[82] The considerable factual differences between *King* and law enforcement's use of FGGSs—primarily that *King* involved a search of a government database and FGGSs involve searches of third-party databases—limit the inferential value of *King* when considering how the Supreme Court will analyze FGGSs.[83]

Given this uncertainty, many commentators believe legislation is necessary to protect genetic information in consumer databases.[84] Proponents of legislative reform tout the need for provisions that create judicial standing and mandate informed consent on behalf of the companies that compile and maintain consumer DNA databases.[85] Recent attempts to ban FGGSs in third-party databases have failed.[86] Currently, Maryland and Montana are the only states that regulate FGGSs: Maryland's scheme requires judicial authorization, while

81. *Id.* at 466, 469–70 (Scalia, J., dissenting) ("If identifying someone means finding out what unsolved crimes he has committed, then identification is indistinguishable from the ordinary law-enforcement aims that have never been thought to justify a suspicionless search.").

82. *King*, 569 U.S. at 466, 467–68 (noting that "while the Court is correct to note . . . instances in which we have permitted searches without individualized suspicion, '[i]n none of these cases … did we indicate approval of a [search] whose primary purpose was to detect evidence of ordinary criminal wrongdoing'" (alterations in original) (quoting Indianapolis v. Edmond, 531 U.S. 32, 38 (2000))).

83. *See id.* at 441; Ford-Monroe, *supra* note 75, at 1729; Selvin, *supra* note 19, at 1026.

84. *E.g.*, Rachel Rosen, Comment, *We Are Family, All My Brothers, Sisters, Murderers and Me: Consent, Privacy, and the Use of Familial DNA in Criminal Investigations*, 90 UMKC L. REV. 191, 217 (2021); Zeevi, *supra* note 12, at 769; Ciera Gonzalez, Note, *Genetic Privacy: Late to the Third Party*, 18 COLO. TECH. L.J. 423, 452 (2020).

85. *E.g.*, Romine, *supra* note 27, at 397; Hill, *supra* note 55, at 1050; Teneille R. Brown, *Why We Fear Genetic Informants: Using Genetic Genealogy to Catch Serial Killers*, 21 COLUM. SCI. & TECH. L. REV. 1, 60–61 (2019).

86. *See* Lindsey Van Ness, *DNA Databases Are Boon to Police but Menace to Privacy, Critics Say*, PEW CHARITABLE TRS. (Feb. 20, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/20/dna-databases-are-boon-to-police-but-menace-to-privacy-critics-say [https://perma.cc/2FS2-2JLP] (discussing bills introduced in Maryland and Utah); Michelle Taylor, *Utah's Commercial Genetic Genealogy Database Bill Fails*, FORENSIC (Mar. 9, 2022), https://www.forensicmag.com/584095-Utah-s-Commercial-Genetic-Genealogy-Database-Bill-Fails/ [https://perma.cc/72QJ-JGNZ] (discussing Utah's proposed legislation).

Montana's requires a traditional warrant.[87] Federally, in November 2019, the DOJ published an interim policy on the use of FGGSs.[88] To limit their application, the DOJ guidance permits FGGSs only "when a case involves an unsolved violent crime and the candidate forensic sample is from a putative perpetrator, or when a case involves . . . the unidentified remains of a suspected homicide victim."[89] Some commentators have called for a national FGGS policy to govern the states.[90] Others promote an alternative model centering on a civilian oversight committee that reviews law enforcement's use of FGGSs pursuant to either the state or federal regulatory scheme or the existing DOJ interim guidelines.[91]

II. ANALYSIS

How the Supreme Court would analyze FGGSs is unknown. The two most relevant cases, *King* and *Carpenter*, were 5–4 decisions with vigorous dissents.[92] This Section will analyze the reasoning in those decisions in search of clues as to how the Court might apply existing doctrine to FGGSs.

87. Jennifer Lynch, *Maryland and Montana Pass the Nation's First Laws Restricting Law Enforcement Access to Genetic Genealogy Databases*, ELEC. FRONTIER FOUND. (June 7, 2021), https://www.eff.org/deeplinks/2021/06/maryland-and-montana-pass-nations-first-laws-restricting-law-enforcement-access [https://perma.cc/9ENK-NPLJ]; MD. CODE. ANN., CRIM. PROC. § 17-102 (West 2022); MONT. CODE ANN. § 44-6-104 (West 2021).

88. *See generally* U.S. DEP'T OF JUST., *supra* note 9 (describing the DOJ's policy on FGGSs).

89. *Id.* at 4 (footnotes omitted).

90. *E.g.*, Alexander (Zan) Eric Newkirk, Note, *Someone Else May Own a Piece of You: Lack of Federal Regulation over Direct-to-Consumer DNA Test Kits*, 20 N.C. J.L. & TECH. ONLINE EDITION 267, 299 (2019); Divya Ramjee & Katelyn Ringrose, *The Challenges of Forensic Genealogy: Dirty DNA, Electronic Evidence, and Privacy Concerns*, 98 DENV. L. REV. 157, 195 (2020).

91. *E.g.*, Craig M. Klugman & Hector F. Rodriguez, *Ethics of Familial Genetic Genealogy: Solving Crimes at the Cost of Privacy*, 22 DEPAUL J. HEALTH CARE L. 67, 88–89 (2021).

92. *See generally* Maryland v. King, 569 U.S. 435 (2013); Carpenter v. United States, 138 S. Ct. 2206 (2018).

A. Maryland v. King *Frames the Debate*

King provides valuable insight into how the Supreme Court might analyze a person's reasonable expectations of privacy in DNA.[93] Because *King* involved a direct match against a DNA profile stored in a government database and not an indirect match in a third-party database, several important differences exist between FGGSs and the Court's analysis in *King*.[94] First, the STR DNA profile analyzed by CODIS in *King* simply revealed a match, unlike the SNP DNA typing stored in consumer databases that could be used to generate physical and personality profiles.[95] Second, whereas a CODIS search can only compare genetic information to existing DNA profiles within government databases, FGGSs can identify exponentially more people by leveraging third-party databases.[96] Third, unlike consumers seeking to compare ancestry or health information, the arrestee in *King* had a diminished expectation of privacy as a result of his arrest.[97]

The Court in *King* distinguished the arrestee's position from the "special needs" exception to the Fourth Amendment that permits law enforcement to engage in "programmatic searches" of law-abiding citizens when the government has substantial interest.[98] This exception permits the government to circumvent the general requirement that a

93. *See King*, 569 U.S. at 462–64 (establishing that law enforcement does not need a warrant to extract a DNA sample from someone who has been arrested on probable cause because the intrusion is minimal and the arrestee has a reduced expectation of privacy).

94. *See* Selvin, *supra* note 19, at 1026.

95. *Compare id.* at 1027 ("Investigators then upload this profile to CODIS, which runs a query against the Offender and Forensic Indexes of every state database and the NDIS, looking for a match."), *with* Abrahamson, *supra* note 42, at 2549–50 (SNPs reveal variations in the genome that can reveal both phenotypic and personality traits). *See generally How DNA Phenotyping Works*, PARABON NANOLABS, https://snapshot.parabon-nanolabs.com/#phenotyping-how [https://perma.cc/92Y2-2HTG] ("DNA phenotyping can generate new leads" and can "translate[] SNP information from an unknown individual's DNA sample into predictions of ancestry and physical appearance traits, such as skin color, hair color, eye color, freckling, and even face morphology.").

96. *See* Lynch, *supra* note 17, at 23; James W. Hazel & Christopher Slobogin, *"A World of Difference"? Law Enforcement, Genetic Data, and the Fourth Amendment*, 70 DUKE L.J. 705, 727 (2021); Schwab, *supra* note 49.

97. *See King*, 569 U.S. at 462 ("The expectations of privacy of an individual taken into police custody 'necessarily [are] of a diminished scope.'" (alteration in original) (quoting Bell v. Wolfish, 441 U.S. 520, 557 (1979))).

98. *Id.* at 462–63 (quoting Chandler v. Miller, 520 U.S. 305, 314 (1997)).

search be the result of "individualized suspicion of wrongdoing" or probable cause.[99] Federal Railroad Administration regulations requiring blood and urine tests of employees after train accidents illustrate this exception.[100] Railroad employees, by working in a heavily regulated industry, have reduced expectations of privacy, and the government has a strong interest in maintaining public safety.[101] Like blood and urine tests for railroad employees, FGGSs involve searching DNA profiles of people who have not been suspected of any wrongdoing.[102] Thus, whether the government's interest in solving cold cases outweighs the privacy interest of suspected-yet-unidentified criminals and innocent consumers who have uploaded their DNA to third-party databases is a critical point of analysis in considering the warrantless validity of FGGSs.

Writing for the majority in *King*, Justice Kennedy emphasized DNA's natural place in law enforcement's history.[103] According to the majority, DNA technology, "one of the most significant scientific advancements of [the] era," is the latest iteration in law enforcement identification technologies, such as photography and fingerprinting.[104] Highlighting the efficacy of DNA-based identification procedures, the Court held the warrantless search of the arrestee's DNA constitutional in light of the arrestee's reduced expectation of privacy balanced against "five discrete governmental interests."[105] Critically, the Court's analysis rested on the premise that "[n]o purpose other than identification is permissible," a premise that was vehemently

99. *See Chandler*, 520 U.S. at 313–14 ("When such 'special needs'—concerns other than crime detection—are alleged in justification of a Fourth Amendment intrusion, courts must undertake a context-specific inquiry, examining closely the competing private and public interests advanced by the parties.").

100. *Id.* at 314–15.

101. *See id.*

102. *See, e.g.*, Hutton, *supra* note 9 (explaining that William Talbott II was convicted on murder based on DNA from his second cousins who "had shared genetic profiles in [a public] database").

103. *See King*, 569 U.S. at 442, 446, 449, 451, 461.

104. *Id.* at 442, 461.

105. Selvin, *supra* note 19, at 1028–29. The five governmental interests are (1) identifying suspects in custody, (2) linking the suspect to past crimes, (3) making decisions regarding bail and "ensuring the suspect shows up for trial," (4) discovering the arrestee's propensity for violence, and (5) freeing anyone "wrongfully imprisoned for the same offense." *Id. See King*, 569 U.S. at 449–61.

challenged by an ideologically diverse dissent.[106] After discussing the precedent of "special needs" searches, which Justice Scalia argued are unrelated to crime detection, the dissent asserted that the Court should never engage in a reasonableness balancing analysis when criminal investigation is at the heart of the matter, such as in *King*.[107] The resolution of this conflict between the majority and dissent depends on the legal definition of "identify."

The majority would have "identify" mean matching a DNA sample from an unsolved crime to an arrestee in custody, while the dissent would have it mean learning information about an arrestee in custody.[108] The conspicuous arrangement of a traditionally Conservative Justice Scalia joined by traditionally Liberal Justices Ginsburg, Sotomayor, and Kagan in a 5–4 decision suggests Fourth Amendment application to the use of genetic information in crime solving may be unpredictable. Since FGGSs of SNP DNA profiles in third-party databases are not in response to an arrest based on probable cause and the scope of the search is exceedingly broad, the Court is unlikely to consider law enforcement's use of FGGSs to generate leads for criminal investigations merely an exercise of identification.

If that is the case, then law enforcement's use of FGGSs would require warrants issued on the basis of probable cause. The problem with this approach, however, is the nature of the FGGS itself. The Supreme Court defines probable cause as "more than bare suspicion," a situation where "[an officer] of reasonable caution" has reason to believe unlawful activity has taken place.[109] This historical standard loses meaning when confronting the reality that FGGSs can identify

106. *King*, 569 U.S. at 465. The dissent, authored by Justice Scalia and joined by Justices Ginsburg, Sotomayor, and Kagan, described the majority opinion as "tax[ing] the credulity of the credulous." *Id.* at 466 (Scalia, J., dissenting). *See also* Daniel G. Klemonski, Oliver K. Natarajan, Samuel H. Studnitzer & Paul M. Sommers, *Ideological Reversal Among Supreme Court Justices*, 5 OPEN J. SOC. SCIS. 290, 292 (2017) (noting Martin-Quinn scores for Justices Ginsburg, Sotomayor, and Kagan are Liberal, and the metric for Justice Scalia is Conservative).

107. *King*, 569 U.S. at 468 (Scalia, J., dissenting).

108. *See id.* at 460–61 (majority opinion); *id.* at 468 (Scalia, J., dissenting).

109. Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (quoting Carroll v. United States 267 U.S. 132, 162 (1925)). The probable cause "standards seek to safeguard citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime" while also "giv[ing] fair leeway for enforcing the law in the community's protection." *Id.* at 176.

more than half of white Americans through a single third-party database.[110] Considering the rapid growth in direct-to-consumer genetic testing and third-party databases, the line between suspicion and probable cause could be obliterated by the near certainty of finding someone who can lead you to the source of the crime scene DNA.[111]

B. Carpenter v. United States *and the Fourth Amendment's Application to Modern Technology*

In holding that the government conducted an unreasonable search by accessing CSLI from "cell phone records that provide a comprehensive chronicle of the user's past movements," the Supreme Court was careful to stress the narrowness of its holding.[112] Hearkening back to an era when the Court was considering the innovations of airplanes and radio, the Court cited the need to proceed cautiously to not "embarrass the future."[113] Each of the four dissenters wrote a separate dissent.[114] Considering the majority's trepidation and the dissents' vigorous opposition to this evolution in modern Fourth Amendment jurisprudence, the Fourth Amendment's application to emerging technologies is anything but clear.[115] The reasoning employed by the majority and dissents, however, sheds light on how the Supreme Court might analyze the Fourth Amendment's application to genetic information in third-party databases.

The Court found that the facts in *Carpenter* fall between two lines of cases, the first involving a person's "expectation of privacy in [the

110. Lynch, *supra* note 17, at 23; Hazel & Slobogin, *supra* note 96.

111. *See supra* notes 47–49 and accompanying text.

112. Carpenter v. United States, 138 S. Ct. 2206, 2211, 2217 (2018). The Court stressed that it did not intend to address any technologies "not before [the Court]" and that there was no intention to "disturb the [third-party doctrine] of *Smith* and *Miller*." *Id.* at 2220.

113. *Id.* at 2220 (quoting Northwest Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).

114. *Id.* at 2223–35 (Kennedy, J., dissenting); *id.* at 2235–46 (Thomas, J., dissenting); *id.* at 2246–61 (Alito, J., dissenting); *id.* at 2261–72 (Gorsuch, J., dissenting).

115. *Compare id.* at 2220 (majority opinion) (stressing the narrowness of the holding), *with id.* at 2223–35 (Kennedy, J., dissenting), *with id.* at 2235–46 (Thomas, J., dissenting), *with id.* at 2246–61 (Alito, J., dissenting), *and id.* at 2261–72 (Gorsuch, J., dissenting) (all dissenters expressing some disapproval of the *Katz* reasonable expectations test vis-à-vis the property-based conception of the Fourth Amendment before *Katz*). *See also* Zeevi, *supra* note 12.

person's] physical location and movements."[116] Describing CSLI as "qualitatively different" than other types of information to which the third-party doctrine had been applied, the Court analogized CSLI to information revealed from an FBI-installed GPS tracking device that monitored a vehicle's movements for twenty-eight days in *United States v. Jones*.[117] The majority deemed CSLI, like GPS data, to be capable of "provid[ing] an intimate window into a person's life, revealing not only [the person's] particular movements, but through them [the person's] 'familial, political, professional, religious, and sexual associations.'"[118]

The window that CSLI opened into an individual's life is analogous to the intimate picture that an SNP DNA profile stored in third-party databases can reveal about consumers, including what a person looks like, what medical conditions they have or are predisposed to develop, and personal traits as obscure as a "preference for cilantro."[119] In addition to the depth of information revealed, the Court considered the breadth of application: If Fourth Amendment protection did not extend to CSLI, law enforcement would have been able to access location information "for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation."[120] Here again, there is a striking similarity to genetic information stored in third-party databases. As of 2019, based on 0.4% of the American adult population having uploaded DNA to GEDmatch, 60% of white Americans could be identified through FGGSs.[121] Should GEDmatch obtain DNA from just 2% of the adult population, law enforcement would be able to identify 90% of white Americans through FGGSs.[122] The similarities between CSLI and SNP DNA profiles in third-party databases—both the depth of information

116. *Carpenter*, 138 S. Ct. at 2209, 2214–15 (majority opinion).
117. *Id.* at 2216–17; *see* United States v. Jones, 565 U.S. 400 (2012).
118. *Carpenter*, 138 S. Ct. at 2217 (quoting *Jones*, 565 U.S. at 415).
119. *See* Abrahamson, *supra* note 42, at 2549; Romine, *supra* note 27, at 379; Carter, *supra* note 12, at 316.
120. *Carpenter*, 138 S. Ct. at 2218.
121. Lynch, *supra* note 17, at 23.
122. *Id.*

revealed and the breadth of application to hundreds of millions of Americans—suggest that the Court would consider SNP DNA profiles "qualitatively different"[123] and worthy of Fourth Amendment protection.

The second line of cases the Court considered in *Carpenter* dealt with the third-party doctrine, or the "line between what a person keeps to himself and what he shares with others."[124] The origin of this line of reasoning is *United States v. Miller*, where an individual being investigated for tax evasion had no expectation of privacy in bank records because he assumed the risk of that information being conveyed to the government by providing the information to the bank.[125] The Court distinguished CSLI from the type of information shared in *Miller*, however, because of the involuntary nature of owning a cell phone in the twenty-first century and the impossibility of using a cell phone without generating location data.[126]

Cell phone users involuntarily sharing CSLI data is distinguishable from eager consumers who take a DNA test and upload their SNP DNA profile to GEDmatch. Whereas the average citizen effectively has no choice but to use a cell phone and generate CSLI,[127] a DNA test is not necessary for modern life. Furthermore, uploading the results to a third-party database is not compulsory. The difference in the voluntariness of these scenarios has led some commentators to believe the third-party doctrine should apply to genetic information revealed during FGGSs, rendering no need for law enforcement to obtain a warrant.[128]

Like *Carpenter*, FGGSs likely involve searching information that is "qualitatively different" from other types of information and is

123. *Carpenter*, 138 S. Ct. at 2216.
124. *Id.*
125. *Id.*; United States v. Miller, 425 U.S. 435, 443 (1976).
126. *See Carpenter*, 138 S. Ct. at 2216–17, 2218–20.
127. *Id.* at 2220.
128. *See, e.g.*, Carter, *supra* note 12; Ford-Monroe, *supra* note 75, at 1731–32 (noting that "the disclosure of genetic information to a genetic testing company" is an "affirmative act" and that, because of the deliberate nature of this disclosure, "civilian DNA databases fit into the third-party doctrine more neatly than even the doctrine's foundational cases").

therefore subject to Fourth Amendment protections.[129] Unlike *Carpenter*, FGGSs, at least those involving GEDmatch, access information that consumers have voluntarily shared with a third party, an "affirmative act" that seemingly removes Fourth Amendment protections.[130] Unclear about the interaction between the third-party doctrine and unique forms of information in the wake of *Carpenter*, a holding that the majority stressed was narrow, courts are left with "amorphous balancing tests" to determine whether Fourth Amendment protection applies.[131] Indeed, Justice Gorsuch asserted that this realm of uncertainty is "where *Katz* inevitably leads."[132]

The solution to this problem, according to Justice Gorsuch, can be found by replacing the *Katz* framework with positive legal rights.[133] Noting that state positive law "often creates rights in both tangible and intangible things," Justice Gorsuch argued this approach could help guide courts "without resort to judicial intuition."[134] Since elected legislatures are more connected to the reasonable expectations of their constituents than the unelected Supreme Court,[135] Justice Gorsuch's positive law approach would likely generate increased stability in Fourth Amendment jurisprudence. This idea is in accord with many commentators' views that there is a critical need for state or federal legislation to define the rights of consumers who have submitted their DNA to third-party databases.[136]

C. Positive Law and FGGSs

Many legal commentators view legislative action as a panacea for the Fourth Amendment's currently unknown applicability to

129. *See Carpenter*, 138 S. Ct. at 2216.
130. Ford-Monroe, *supra* note 75, at 1731.
131. *Carpenter*, 138 S. Ct. at 2220; *id.* at 2267 (Gorsuch, J., dissenting).
132. *Id.* at 2267 (Gorsuch, J., dissenting).
133. *See id.* at 2265.
134. *Id.* at 2270.
135. *See id.* at 2266 ("As a result, [the *Katz* reasonable expectations of privacy framework] has yielded an often unpredictable—and sometimes unbelievable—jurisprudence. . . . Yet rather than defer to that as evidence of the people's habits and reasonable expectations of privacy, the Court substituted its own curious judgment.").
136. *See supra* note 84 and accompanying text.

FGGSs.[137] This approach empowers representative bodies to moderate law enforcement, safeguard citizens' privacy rights, and guide judicial application of the Fourth Amendment to FGGSs within the existing *Katz* framework. For example, a state legislature could define the conditions in which a citizen has a reasonable expectation of privacy in a commercially generated SNP DNA profile. Such a legal determination would mitigate the need for an "amorphous" judicial balancing test.[138]

An expectation of privacy defined by statute could help guide companies in creating informed consent provisions, possibly by taking consumers to a separate web page that explains the implications of sharing their DNA, thus allowing law enforcement to avoid the warrant requirement if consumers have consented to participate in an FGGS program.[139] Consumers sharing their DNA profiles with the knowledge that they are potentially participating in criminal investigations would arguably constitute a legitimate exercise of the third-party doctrine because it is an "affirmative act," unlike the compulsory CSLI data collection in *Carpenter*.[140] It is plausible that laws defining an expectation of privacy and mandating informed consent provisions by companies compiling and managing DNA databases could bring FGGSs within the third-party doctrine developed in *Miller* and within the *Katz* reasonable expectation of privacy framework, assuming that society is willing to accept such laws as reasonable.[141]

The situation becomes more complex, however, when considering the legal ramifications of DNA as property.[142] Since DNA is not singularly possessed, but instead "immutably shared" with family

137. *See, e.g., id.*

138. *See Carpenter*, 138 S. Ct. at 2267, 2270 (Gorsuch, J., dissenting).

139. *See* Hill, *supra* note 55, at 1070 ("To establish balance between privacy and law enforcement interests, federal and state legislators should require DTC companies to include an explicit and informative option for individuals to opt out of law enforcement access while signing up for the service.").

140. *See* Ford-Monroe, *supra* note 75, at 1731–32; *Carpenter*, 138 S. Ct. at 2220 (categorizing CSLI as not voluntarily shared because cell phones are "indispensable to participation in modern society").

141. *See* United States v. Miller, 425 U.S. 435, 442 (1976); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

142. *See* Ram, *supra* note 20.

members, the traditional notion of consent is frustrated by the realities imposed by biology.[143] Indeed, any legislature attempting to define a citizen's expectation of privacy in a commercially generated SNP DNA profile stored in third-party databases must address what expectation of privacy the relatives of the DNA profile's owner have in the genetic information.[144] Unlike traditional property rights, defined by the right to exclude others from using the property, relatives cannot exclude third parties from examining portions of their DNA given away without their consent.[145]

As of 2018, five states—Alaska, Colorado, Florida, Georgia, and Louisiana—passed laws making genetic information personal property.[146] These exclusive property rights are a step towards clarifying a murky legal area, but the simple reality remains: An individual can be identified by law enforcement based on an SNP DNA profile from as many as 800 different relatives.[147] As states begin to regulate FGGSs, they might need to conceptualize property rights in DNA through novel analogs to balance consumers' privacy interests against the government's interest in solving crime.[148]

143. *Id.* at 903, 906.

144. *See* Hillary L. Kody, Note, *Standing to Challenge Familial Searches of Commercial DNA Databases*, 61 WM. & MARY L. REV. 287, 318 (2019) (arguing that an "expectation of privacy extends to family members who are unable to disconnect their DNA from their family members' DNA in third-party databases").

145. *See* Jessica L. Roberts, *Progressive Genetic Ownership*, 93 NOTRE DAME L. REV. 1105, 1120 (2018) (providing examples of the right to exclude in the typical property context); *id.* at 1130 (explaining that, primarily through informed consent, "[i]ndividuals enjoy a limited right to exclude pertaining to their genetic data").

146. ALASKA STAT. § 18.13.010(a)(2) (2022); COLO. REV. STAT. § 10-3-1104.7(1)(a) (2022); FLA. STAT. ANN. § 760.40(1)(c) (West 2022); GA. CODE ANN. § 33-54-1(1) (2022); LA. STAT. ANN § 22:1023(E) (2022). It is possible that more states could follow suit, since "legislators in South Dakota, Alabama, Massachusetts, and Texas have introduced bills that would make a person's genetic information or DNA sample her property." Roberts, *supra* note 145, at 1128.

147. Schwab, *supra* note 49. As Ram explains, the "shared nature [of genetic information] renders existing rules a poor fit for adjudicating claims to genetic information." Ram, *supra* note 20, at 899. These "existing rules" are insufficient "to address to the more numerous stakeholders that have an interest in a single cell's genetic information as a matter of biological fact." *Id.*

148. *See, e.g.*, Ram, *supra* note 20, at 918–19 (suggesting lawmakers look to the law of tenancy by the entirety as a possible model for how to conceptualize DNA as property); Roberts, *supra* note 145, at 1156–67 (noting that genetic data is similar to land in that "[b]oth are unique, both are inheritable, and both are tied to family and community," and suggesting that the theory of progressive property could help expand and refine the conceptualization of genetic information).

III. PROPOSAL

Some commentators have declared it is time for a universal forensic database in the United States.[149] Proponents argue that society is moving towards "an underregulated, de facto universal database," where law enforcement exploits databases like GEDmatch and FamilyTreeDNA without oversight.[150] Due to the zealousness with which Americans generally guard their personal liberties, the likelihood of a government-operated universal forensic database is remote. Thus, society must deal with the patchwork status quo and the likelihood that non-government, third-party DNA databases will continue to accumulate Americans' DNA.[151] Even modest growth from the status quo could render nearly all Americans identifiable through FGGSs.[152] After examining the difficulties that the existing legal framework has in accommodating FGGSs, this proposal provides a solution that stabilizes Fourth Amendment jurisprudence and discourages disparate and competing state regulatory regimes.

A. Probable Cause and Third-Party DNA Databases

The first way a Fourth Amendment search can be valid is through a judicially sanctioned warrant based on probable cause.[153] As defined by the Supreme Court, probable cause requires more than suspicion; the officer must have reason to believe some offense has been

149. *E.g.*, J.W. Hazel, E.W. Clayton, B.A. Malin & C. Slobogin, *Is It Time for a Universal Genetic Forensic Database?*, 362 SCI. 898, 898 (2018); Michael Seringhaus, Opinion, *To Stop Crime, Share Your Genes*, N.Y. TIMES (Mar. 14, 2010), https://www.nytimes.com/2010/03/15/opinion/15seringhaus.html [https://perma.cc/K7UH-6V2T].

150. J.W. Hazel, E.W. Clayton, B.A. Malin & C. Slobogin, Response, *Risk of Compulsory Genetic Databases*, 363 SCI. 938, 939 (2019).

151. More DTC DNA tests were sold in 2018 than all prior years combined and that if such growth continues, the "four leading commercial ancestry and health databases" could house DNA profiles for more than 100 million consumers. Regalado, *supra* note 39.

152. *See* Lynch, *supra* note 17, at 23.

153. *See* U. S. CONST. amend. IV; Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." (footnotes omitted)).

committed.[154] It is difficult to imagine a commonsense application of this concept to FGGSs, a process in which law enforcement is searching potentially millions of DNA profiles to find genetic similarities to source DNA from a crime scene.[155]

What is the meaning of probable cause in this scenario? If third-party databases grow to the extent that finding an identifiable match is a near certainty, does that automatically clear the probable cause hurdle? In 2019, after GEDmatch stopped automatically sharing its information with law enforcement and began giving users an FGGS opt-in option, a federal judge in Florida granted a warrant to search the nearly one million DNA profiles who had chosen not to share their profiles with law enforcement.[156] Despite the potential for this warrant to set a precedent, outrage from privacy advocates indicates this practice will be hotly contested.[157] On a fundamental level, an FGGS warrant contravenes the Fourth Amendment's prohibition against general warrants, which were historically limited in scope only by the executing officer's discretion.[158] Since searching millions of profiles reflects no limitation in scope, the existing warrant system is ill-equipped to control the use of FGGSs.

B. The Katz *Framework: A Balancing of Competing Interests*

If there is no judicially sanctioned warrant, a law enforcement search can be valid when it is reasonable.[159] If a citizen does not have a reasonable expectation of privacy in the place or activity in question, then a search not does not violate the Fourth Amendment so long as it is "reasonable in its scope and manner of execution."[160] If the

154. Brinegar v. United States, 338 U.S. 160, 175–76 (1949).

155. *But see* Hill & Murphy, *supra* note 53 (describing how a warrant issued by a Florida judge permitted a detective to search nearly one million DNA profiles of users who had chosen not to share their genetic information with law enforcement).

156. *Id.*

157. *See* Cassie Martin, *Why a Warrant to Search GEDmatch's Genetic Data Has Sparked Privacy Concerns*, SCIENCENEWS (Nov. 12, 2019, 4:07 PM), https://www.sciencenews.org/article/why-warrant-search-gedmatch-genetic-data-has-sparked-privacy-concerns [https://perma.cc/5HE2-4Z8D].

158. *See* Boyd v. United States, 116 U.S. 616, 624–25 (1886).

159. Maryland v. King, 569 U.S. 435, 448 (2013); *see also* U. S. CONST. amend. IV.

160. *King*, 569 U.S. at 448.

individual does have a legitimate expectation of privacy, the reasonableness of the warrantless search or seizure will depend on a balancing of the individual's expectation of privacy against the government's interest.[161]

1. The Government Has an Exceptionally Strong Interest in Using FGGSs

Protecting citizens from criminal activity and delivering justice to the perpetrators and victims of violent crime are indispensable government functions. With more than 200,000 cold cases in 2019,[162] the United States needs technologies to solve crimes and reduce criminality. As evidence of the power of FGGSs, Cece Moore, the prominent genetic genealogist who identified William Earl Talbott II as the source of the DNA found at two Seattle murders, has been responsible for "over one positive identification per week" in her time at Parabon.[163]

There is no inherent bottleneck preventing widespread use of this technology and no issue of resource scarcity or shortage of skilled labor.[164] If more people develop the ability to build family trees by analyzing genetic information and third-party databases continue sharing genetic information with law enforcement, FGGSs should continue to solve cold cases that have haunted victims' families for years.[165] FGGSs thus amount to a critical addendum to the generational breakthrough of law enforcement's use of DNA, which was instituted

161. *See, e.g.*, *id*. at 449–52 (assessing the reasonableness of a government's warrantless use of a buccal swab to test an arrestee's DNA by weighing the government's interest served by the Maryland law authorizing the buccal swab against the individual's expectation of privacy).

162. George M. Dery III, *Can a Distant Relative Allow the Government Access to Your DNA?*, 10 HASTINGS SCI. & TECH. L.J. 103,144 (2019).

163. *About Parabon NanoLabs*, *supra* note 3.

164. *Cf.* Regalado & Alexander, *supra* note 5 (describing how Cece Moore, "[l]ike other prominent figures in the genealogy community" is "self-taught").

165. *See SeaTac Man Convicted*, *supra* note 2 (quoting the older brother of the murdered Tany Van Cuylenbord as being thankful for this technology: "It feels great to have some answers. We don't have all the answers, but we have a lot more than we had for 31 years").

through CODIS in 1998.[166] Although familial searches for partial DNA matches have been done in CODIS "since the early 2000s," the SNP DNA profiles in third-party databases offer the distinct advantage of providing considerably more information than the STR DNA profiles used in CODIS, in turn "making familial searches easier."[167] Additionally, since the DNA in CODIS comes only from arrestees or convicts, third-party databases increase both the size and diversity of law enforcement's access to DNA evidence for partial matching.[168]

The state interest in promoting justice and public safety by removing perpetrators of violent crimes from the general population is greater than the state interest in *King*.[169] Although identification may allow police to solve a cold case, as in *King*, the cold-case breakthrough was merely incidental to the core administrative function of collecting DNA for identification purposes.[170] In contrast, solving cold cases is the primary function of FGGSs.[171] The weight of the legitimate government interest in FGGSs is increased by the fact that unidentified crime scene DNA may belong to rapists and murderers. Short of protecting the country against foreign aggression, it is difficult to imagine a stronger public policy interest than solving and preventing the most heinous criminal acts, aims which are enhanced by FGGSs.

166. *See* Press Release, FBI National Press Office, The FBI's Combined DNA Index System (CODIS) Hits Major Milestone (May 21, 2021), https://www.fbi.gov/news/press-releases/the-fbis-combined-dna-index-system-codis-hits-major-milestone [https://perma.cc/H72R-PL68].

167. Ford-Monroe, *supra* note 75, at 1721–22.

168. *See id.* at 1722.

169. *King*, 569 U.S. at 449. "The legitimate government interest served by the Maryland DNA Collection Act is one that is well established: the need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody." *Id.*

170. *Id.* at 441 (noting that the officers who took the swab were complying with a Maryland law that only authorized DNA collection for identification purposes).

171. *See* U.S. DEP'T OF JUST., *supra* note 9 ("Forensic genealogy is law enforcement's use of DNA analysis combined with traditional genealogy research to generate investigative leads for unsolved violent crimes.").

2. DNA Consumers Have an Expectation of Privacy in Their Genetic Information

Unlike the STR DNA profiles used in CODIS, which "the [Supreme Court] and the medical community at large have referred to . . . as 'nonprotein coding junk,'" SNP DNA profiles in third-party databases reveal intimate details about the source of the genetic information, including physical traits, medical traits, and possibly even personality traits.[172] The government accesses this genetic information through different means. In CODIS, the government accesses genetic information of convicts or arrestees.[173] In either scenario, the source of the genetic information has a reduced expectation of privacy.[174] Compared with the arrestee in *King*, the consumers uploading their SNP DNA profiles to a third-party DNA database have a greater expectation of privacy. If applicable, however, the third-party doctrine, first articulated in *Miller*,[175] would undermine this expectation and swing the balancing test in favor of the government.

After *Carpenter*, it is unclear whether the third-party doctrine would apply to genetic information voluntarily uploaded to third-party databases. Some argue that the doctrine should apply, rendering the SNP DNA profiles unprotected by the Fourth Amendment.[176] Yet it is possible that this information falls outside the doctrine's purview because it is "qualitatively different" like the CSLI in *Carpenter*.[177] Additionally, informed consent provisions or policies, like the one

172. *See* Abrahamson, *supra* note 42, at 2547 (quoting *King*, 569 U.S. at 445) (STR DNA typing is considered "junk" because it does not contain information "that is 'presently recognized as being responsible for trait coding'" (quoting United States v. Kincade, 379 F.3d 813, 818 (9th Cir. 2004))); Romine, *supra* note 27, at 379.

173. *See Frequently Asked Questions on CODIS and NDIS*, *supra* note 27.

174. *King*, 569 U.S. at 463 ("Once an individual has been arrested on probable cause for a dangerous offense that may require detention before trial, however, his or her expectations of privacy and freedom from police scrutiny are reduced.").

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

176. *E.g.*, Carter, *supra* note 12.

177. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214, 2216 (2018); Abrahamson, *supra* note 42, at 2539.

GEDmatch implemented in May of 2019,[178] could play a significant role in salvaging the third-party doctrine's application to genetic information in third-party databases. There is, however, a critical flaw in this reasoning. Even with well-constructed informed consent measures in place, it is virtually impossible to obtain consent from hundreds of relatives an individual would make identifiable by opting in to share a DNA profile with law enforcement.[179] If informed consent were required of all potentially identifiable individuals, GEDmatch would need to contact tens of millions of Americans.[180] Indeed, assuming no one had opted to share data since GEDmatch changed its policy and that each SNP DNA profile could identify 200 relatives (the lower bound for that variable), then at least thirty-seven million relatives would be identifiable.[181]

Because of the "qualitatively different"[182] nature of DNA, principally that it is deeply revealing and communally shared, this Note concludes that the third-party doctrine does not apply to genetic information voluntarily uploaded to third-party databases. Informed consent procedures that permit consumers to affirmatively choose to cooperate with law enforcement may bring the uploaded DNA within the third-party doctrine, but that analysis cannot be supported based on *Carpenter*'s reasoning alone and dodges the intractable question of what right a relative has in the uploader's SNP DNA profile.[183]

178. *See generally* Natalie Ram, *The Genealogy Site that Helped Catch the Golden State Killer Is Grappling with Privacy*, SLATE (May 29, 2019, 7:30 AM), https://slate.com/technology/2019/05/gedmatch-dna-privacy-update-law-enforcement-genetic-geneology-searches.html [https://perma.cc/W86S-PM4Z] (discussing GEDmatch changing its terms of service).

179. Selvin, *supra* note 19, at 1024–25.

180. *See supra* notes 47–49 and accompanying text.

181. This calculation is based on the conservative estimate that everyone has around 200 third cousins and the 185,000 GEDmatch users who chose to opt in to the policy change in 2019. Romine, *supra* note 27, at 373; Hill & Murphy *supra* note 52.

182. *See Carpenter*, 138 S. Ct. at 2216–17 (holding that the third-party doctrine applied to telephone numbers and bank records but did not apply to the "qualitatively different" information of cell-site records).

183. *See generally* Ram, *supra* note 20; *Carpenter*, 138 S. Ct. at 2219–21 (focusing on the nature of the CSLI and the lack of voluntary submission of the information). Although it is true that in this case there would be voluntary compliance on behalf of the single individual, there is no practical way to obtain consent on behalf of that individual's relatives. Ram, *supra.*

Subsequently, no clear indication exists at this time as to whether the government's interest in solving cold cases and preventing serial perpetrators outweighs the privacy interest of an individual and the individual's relatives in their own DNA. Additionally, because law enforcement uses FGGSs to detect crime, no basis exists for the "special needs" exception to apply.[184] If the ideologically diverse dissent in *King*, a 5–4 case, became law, then the entire balancing inquiry would be inappropriate because of the investigatory nature of FGGSs, and the warrantless search would become unconstitutional.[185]

C. Positive Law Can Guide the Judiciary

Dissenting in *Carpenter*, Justice Gorsuch expressed his disapproval of the third-party doctrine and asserted that the Court "has never offered a persuasive justification" for the theory.[186] Regarding the balancing of government and private interests, Justice Gorsuch considered the exercise "little more than the product of judicial intuition."[187] Confronted with the prospect of an ad hoc balancing of abstract interests for each emerging technology, this Note asserts that Justice Gorsuch has the superior strategy for navigating the unknown: Let legislatures define citizens' expectation of privacy in genetic information. Judges can then "decide cases based on 'democratically legitimate sources of law'" rather than "personal policy preferences" or interpretations of abstract legal theory.[188]

1. The Limitations of a State-Based Solution

In 1932, Justice Brandeis famously pronounced that "[i]t is one of the happy incidents of the federal system that a single courageous State

184. *See* Chandler v. Miller, 520 U.S. 305, 314 (1997) (noting that the "[s]pecial needs" exception applies when there are "concerns other than crime detection"); *"Special Needs" Exception to the Warrant Requirement*, U.S. DEP'T OF JUSTICE OFF. OF JUST PROGRAMS, https://www.ojp.gov/ncjrs/virtual-library/abstracts/special-needs-exception-warrant-requirement [https://perma.cc/C3R4-J9HP].

185. *See* Maryland v. King, 569 U.S. 435, 468 (2013) (Scalia, J., dissenting).

186. *Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting).

187. *Id.* at 2267.

188. *Id.* at 2267–68 (quoting Todd E. Pettys, *Judicial Discretion in Constitutional Cases*, 26 J.L. & POL. 123, 127 (2011)).

may, if its citizens choose, serve as a laboratory[] and try novel social and economic experiments without risk to the rest of the country."[189] This pronouncement is particularly valuable in the twenty-first century where technological evolution and social change occur at a blistering pace. It implies that states should define when and where its citizens maintain a "reasonable expectation of privacy," updating Justice Harlan's two-pronged Fourth Amendment inquiry to accommodate a digital world.[190] Compared with an abstract expectation of privacy that society considers reasonable,[191] legislators can more precisely define such an expectation based on what their constituents tell them. Such a change would increase the flexibility of the *Katz* framework—flexibility that is needed as emerging technologies, like DNA testing in *King* and CSLI in *Carpenter*,[192] will continue to challenge the established framework of Fourth Amendment jurisprudence.

There is a significant problem, however, with states defining the expectation of privacy for commercial DNA in third-party databases. Although some states have attempted to ban FGGSs altogether, a policy decision that is a viable expression of democratic will, states that choose to establish programs for regulating FGGSs could encounter complicated questions regarding choice of law and jurisdiction.[193] For example, which state law should govern FGGS procedure? Should it be the state where the investigation began or, if different, the state where the suspect's relative lives? What happens if the uploader of the SNP DNA profile consented to law enforcement participation in a state that has an FGGS program but subsequently moved to a state that prohibits FGGSs? These questions point to the simple answer at the heart of a complex legal inquiry: Neither DNA

189. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

190. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

191. *See id.*

192. *See generally Carpenter*, 138 S. Ct. 2205; Maryland v. King, 569 U.S. 435 (2013).

193. *See* Van Ness, *supra* note 86 (discussing a challenge to a warrant based on jurisdictional grounds).

nor third-party online databases can realistically be bound by state jurisdictions. Thus, FGGSs should be regulated at the federal level.

2. The Unlikely Prospect of a Comprehensive Federal Solution

The DOJ's interim policy for FGGSs gets to the heart of the controversy in announcing its purpose to "promote the reasoned exercise of investigative, scientific, and prosecutorial discretion" in the use of this technology.[194] These guidelines, which recognize both the state's strong interest in solving crimes and the invasion of privacy to the consumer, are intended to prevent the unlimited discretion latent in the general warrants of the colonial era.[195] For example, the DOJ interim guidelines limit the application of FGGSs to homicide and sex crimes, assuring that the invasion of individual privacy rights will occur only in the presence of exceptional governmental interest.[196] Additionally, they limit application of the technology to generating investigatory leads, ensuring that suspects will not be arrested on dubious, abstract evidence.[197]

The policy currently applies to "DOJ agencies[] and state or local agencies that receive federal funding to complete genetic genealogy searches."[198] These interim guidelines are a "solid first attempt" at bringing some order to the chaos, but they fail to protect users who do not consent to cooperate with law enforcement and citizens "whose genetic information is exposed by their relatives."[199] Since the interim guidelines do not adequately address all relevant stakeholders in the ecosystem, this Note considers the guidelines merely the first iteration of federal FGGS regulation. Due to the novelty of the technology and the political divisiveness surrounding police reform, it is difficult to envision Congress promulgating a comprehensive regulatory scheme

194. U.S. DEP'T OF JUST., *supra* note 9, at 1.
195. *See id.*; Boyd v. United States, 116 U.S. 616, 624–25 (1886).
196. U.S. DEP'T OF JUST., *supra* note 9, at 4 & n.15.
197. *Id.* at 4; Carter, *supra* note 12, at 330.
198. Schwab, *supra* note 49.
199. *Id.*

in the near future. As such, the DOJ's interim policy will likely become more influential.

3. The Middle Path

Since FGGSs need a federal solution and a comprehensive legislative regulatory scheme is not imminent, this Note proposes that state legislatures establish civilian forensic science oversight boards, like Massachusetts's Forensic Science Oversight Board,[200] that can independently monitor the use of FGGS technology. The oversight boards could oversee the implementation of the DOJ interim guidelines, work to minimize conflict of law issues, and generally encourage a uniform national practice in a constitutionally opaque endeavor. Critically, such oversight bodies must be independent from law enforcement so they can appropriately moderate the tension between law enforcement and citizen privacy. Additionally, these bodies should regularly report FGGS findings to the legislature, the branch of government closest to citizens' expectations of privacy.

Like the Massachusetts model, state forensic science oversight boards should be composed of scientists, mathematicians, and legal professionals dedicated both to prosecution of crime and criminal defense.[201] A diverse compilation of civilian experts would provide the internal checks and balances necessary to moderate decision making. A legislatively created civilian forensic science oversight committee is more apt to answer inevitable questions: Should the state use this technology to solve an active case in contravention of the DOJ interim

200. MASS. GEN. LAWS ANN. ch. 6, § 184A (West 2022); *Forensic Science Oversight Board*, MASS.GOV, https://www.mass.gov/forensic-science-oversight-board [https://perma.cc/X42G-RVPJ]. Two other models are the Biometrics and Forensics Ethics Group in the United Kingdom, which "has oversight into the ethical issues surrounding familial searching," and the Interdisciplinary Familial Search Committee in California, which "reviews law enforcement requests" for familial searches. Klugman & Rodriguez, *supra* note 91, at 88–89 ("These models may provide a national approach to familial genetic searching of law enforcement, commercial, and public DNA databases.").

201. *See Forensic Science Oversight Board Members*, MASS.GOV, https://www.mass.gov/service-details/forensic-science-oversight-board-members [https://perma.cc/PW48-WQS4].

guidelines?[202] Should the state cooperate with other state FGGS programs to overcome complex choice of law problems? Should state forensic science oversight boards proliferate, they could work with the national government to develop a permanent federal solution.

CONCLUSION

Warrantless searches of genetic information in third-party databases challenge the Fourth Amendment framework established by Justice Harlan's concurrence in *Katz*.[203] In 2013, the Supreme Court denied Fourth Amendment protection to genetic information in *King* when it found that the state interest in identifying an arrestee in custody outweighed the individual's diminished reasonable expectation of privacy.[204] In 2018, the Supreme Court refused to extend the third-party doctrine to CSLI, thereby granting Fourth Amendment protection to the revealing information generated by modern technology.[205] The Court reasoned that this information was "qualitatively different" than information in previous Fourth Amendment analyses and that cell phones were an indispensable part of modern life, leaving the consumer with no choice but to participate in the data collection.[206]

Applying *Carpenter*'s reasoning, the Supreme Court would likely analogize SNP DNA profiles in third-party databases as "qualitatively different," but, unlike cell phones, uploading the results of a direct-to-consumer DNA test is demonstrably not an indispensable aspect of modern life. Lacking a clear indication of what *Carpenter* means for FGGSs, this Note analyzed FGGSs under the *Katz* balancing test, a process which fails to yield a clear, convincing answer. As an alternative to the *Katz* balancing test, Justice Gorsuch's positive law

202. *See* Carter, *supra* note 12, at 330 (noting that the DOJ guidelines only permit FGGSs "after other databases like CODIS have been searched and other traditional investigation methods have been deployed").

203. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

204. Maryland v. King, 569 U.S. 435, 465 (2013).

205. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214, 2216 (2018).

206. *Id.* at 2216–20.

solution can provide Fourth Amendment jurisprudence the flexibility needed to adapt to future emerging technologies.[207] A state-based positive law solution for FGGSs, however, would create intractable problems related to choice of law and jurisdiction.

Since a federal positive law solution is necessary to comprehensively regulate FGGSs but difficult to accomplish politically, this Note proposes that state-created interdisciplinary forensic science oversight boards, modeled on the Massachusetts Forensic Science Oversight Board, should guide FGGS policy consistent with the DOJ interim guidelines published in 2019. As the interim guidelines evolve in response to stakeholder input, the state oversight boards will be in the best position to oversee the implementation of new regulations and participate in the creation of a comprehensive federal regulatory scheme for the forensic use of genetic information in third-party databases.

207. *See id.* at 2261–72 (Gorsuch, J., dissenting).