Hastings Law Journal

Volume 72 | Issue 6 Article 5

8-2021

Why Familial Searches of Civilian DNA Databases Can and Should Survive Carpenter

Jasper Ford-Monroe

Notes

Why Familial Searches of Civilian DNA Databases Can and Should Survive *Carpenter*

JASPER FORD-MONROE[†]

Over the past few years, a powerful new forensic technique has emerged. By uploading DNA from a crime scene to a civilian DNA database, such as GEDmatch, investigators can discover the genetic relatives of the perpetrator and thereby track down the perpetrator himself. This procedure is known as forensic genetic genealogy searching (FGGS), and in under three years it has cracked numerous decades-old cases once thought to be unsolvable.

Concerned about genetic privacy and discrimination, most legal commentators have thus far confronted FGGS with raised hackles. They either argue FGGS is a Fourth Amendment search under Carpenter*, or that it escapes* Carpenter *but ought to be severely restricted or prohibited by statute.*

This Note attempts to show both that FGGS is not a Fourth Amendment search under Carpenter*, and that public policy supports its use to the fullest practicable extent. On the doctrinal side, FGGS is distinguishable on every point from the location information at issue in* Carpenter*. On the practical side, FGGS is of immense forensic value, and the existence of sensible regulatory restrictions should serve to assuage popular fears.*

[†] J.D. 2021, University of California, Hastings College of the Law. The Author would like to thank Professor Binyamin Blum and Oliver Hamilton, as well as the rest of the HLJ team.

TABLE OF CONTENTS

INTRODUCTION

Since the United States Supreme Court revised the third-party doctrine in its 2018 *Carpenter v. United States*[1] decision, many commentators have speculated about whether the decision applies to other kinds of emerging technology.[2] One such technology is the civilian DNA database. Such databases now boast millions of users who have submitted their DNA.[3]

Law enforcement in some states has recently begun to use one of these databases, GEDmatch, to conduct familial searches for unidentified offenders.[4] The technique of conducting familial searches through civilian databases has no universally agreed-upon name at present. This Note will use the Department of Justice's term, "forensic genetic genealogical DNA analysis and searching," or "FGGS."[5]

Up until now, commentators have argued that FGGS can or should be analogized to the location data collection in *Carpenter*.[6] For example, they have suggested the high volume of data inherent in a person's DNA profile is analogous to the high volume of location data involved in *Carpenter*.[7] They have also voiced concerns about the sensitive personal information available in DNA, such as a person's propensity for genetic-based disease.[8]

However, DNA only reveals information about a person's biological being at time of birth, and cannot shed any light on a person's actions, associations, or how they have chosen to live their life more generally.[9] By contrast, the location information at stake in *Carpenter* reveals a person's day-to-day actions and

---

1. Carpenter v. U.S., 138 S. Ct. 2206 (2018).

2. *See, e.g.*, Eunice Park, *Objects, Places and Cyber-Spaces Post-Carpenter: Extending the Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA*, 21 YALE J. L. & TECH. 1 (2019); Paul Ohm, *The Many Revolutions of Carpenter*, 32 HARV. J. L. & TECH 357 (2019).

3. *Company Facts,* ANCESTRY, https://www.ancestry.com/corporate/about-ancestry/company-facts (last visited July 31, 2021) (over 20 million people in network); *About,* 23ANDME, https://www.23andme.com/about (last visited July 31, 2021) (more than 12 million testing kits sold).

4. Robert Gearty, *DNA, Genetic Genealogy Made 2018 the Year of the Cold Case: "Biggest Crime-Fighting Breakthrough in Decades*," FOX NEWS (Dec. 19, 2018), https://www.foxnews.com/us/dna-genetic-genealogy-made-2018-the-year-old-the-cold-case-biggest-crime-fighting-breakthrough-in-decades.

5. U.S. DEP'T OF JUST., INTERIM POLICY: FORENSIC GENETIC GENEALOGICAL DNA ANALYSIS AND SEARCHING 1 (2019), https://www.justice.gov/olp/page/file/1204386/download.

6. *Compare* George M. Dery III, *Can a Distant Relative Allow the Government Access to Your DNA? The Fourth Amendment Implications of Law Enforcement's Genealogical Search for the Golden State Killer and Other Genetic Genealogy Investigations*, 10 HASTINGS SCI. & TECH. L.J. 103, 121–28 (2019) (*Carpenter* applies to FGGS) *with* Antony Barone Kolenc, *"23 and Plea": Limiting Police Use of Genealogy Sites After Carpenter v. United States*, 122 W. VA. L. REV. 53, 100–01 (2019) (*Carpenter* does not apply to FGGS, but FGGS should be restricted by other means), *and* Alexandra Nieto, *Familial Searching: How Implementing Minimum Safeguards Ensures Constitutionally-Permissible Use of This Powerful Investigative Tool*, 40 CARDOZO L. REV. 1765 (arguing in favor of familial searching, but only briefly mentioning civilian databases and *Carpenter*).

7. Kolenc, *supra* note 6, at 97.

8. *Id.* at 73–74.

9. *See, e.g.*, *Ancestry + Traits Service*, 23ANDME, https://www.23andme.com/dna-ancestry (last visited July 31, 2021).

thereby intrudes into their private affairs.[10] The rationale of *Carpenter*, thus, does not seem to extend to FGGS.

Likewise, FGGS is distinguishable from a public policy standpoint. The benefits of its use are enormous, and its nature is such that certain simple safeguards will minimize the likelihood of abuse. For the foregoing reasons, this Note expounds on a position contrary to that of the prevailing literature: that FGGS is not a Fourth Amendment search subject to the warrant requirement, and public policy supports its status as such.

Part I of this Note reviews the process of FGGS and the ways in which it is currently regulated. Specifically, Part I reviews the facts and holdings of *Carpenter* and the relevant aspects of *Maryland v. King*, the most recent U.S. Supreme Court case about DNA identification. Part II applies the rationale of *Carpenter* and *King* to the practice and procedure of FGGS, and concludes that FGGS, for Fourth Amendment purposes, does not constitute a search. It also argues that public policy considerations favor the continued use of FGGS. Part III speculates how FGGS may be performed in the future and offers recommendations to encourage and expand the safe and effective use of FGGS.

I. BACKGROUND

DNA is a molecule that determines biological traits, found in the cells of all living things.[11] Each person has a different pattern of DNA.[12] Because of this uniqueness, DNA can be used in forensics in much the same way as fingerprints, and indeed with an even higher rate of success.[13] DNA has been so used since the late 1980s.[14]

Civilian DNA databases can be divided into two groups: commercial and open.[15] The two largest commercial DNA databases, Ancestry and 23andMe, have (to date) 20 million and 12 million customers, respectively.[16] These sites, and other "direct-to-customer" databases, work in much the same way. The customer purchases a DNA collection kit and sends the company a DNA sample, typically saliva.[17] The company then analyzes the customer's DNA and gives

10. *Carpenter*, 138 S. Ct. at 2217.

11. LEARN.GENETICS, *What are DNA and Genes?*, https://learn.genetics.utah.edu/content/basics/dna. For more basic scientific background on DNA, *see generally* LEARN.GENETICS, *Basic Genetics*, https://learn.genetics.utah.edu/content/basics.

12. LEARN.GENETICS, *supra* note 11.

13. *E.g.*, John K. Roman, Shannon Reid, Jay Reid, Aaron Chalfin, William Adams & Carly Knight, *The DNA Field Experiment: Cost-Effectiveness Analysis of the Use of DNA in the Investigation of High-Volume Crimes*, URBAN INST. 3 (June 16, 2008), https://www.urban.org/research/publication/dna-field-experiment/view/full_report.

14. *See*, *e.g.*, Andrews v. State, 533 So. 2d 841, 842 (Fla. Dist. Ct. App. 1988) (ruling on admissibility of DNA evidence), *abrogated by* Hadden v. State, 690 So. 2d 573 (Fla. 1997).

15. U.S. DEP'T OF JUST., *supra* note 5, at 3.

16. ANCESTRY, *supra* note 3.

17. *See, e.g.*, *How it Works,* 23ANDME, https://www.23andme.com/howitworks/.

the customer information based on that analysis, including ethnic background, genetic relations to other users of the service, and genetic traits.[18] These include phenotypic traits, such as eye and hair color, as well as genotypic traits, such as disease propensities.[19]

Open DNA databases, by contrast, do not perform their own DNA testing, but allow users to upload their data from different commercial databases.[20] The most prominent open database is GEDmatch, with over 1.4 million users at last report.[21]

FGGS is a process by which law enforcement makes use of these civilian databases. This Note begins by detailing the current state of FGGS, then moves to relevant case law, focusing on *Carpenter* and *King*.

A. THE CURRENT PRACTICAL AND LEGAL STATE OF FGGS

This Subpart begins by explaining the FGGS process and the fruits of its use. It then moves on to discuss the current restrictions on FGGS.

1. FGGS Procedure

FGGS is performed as follows: first, the government contracts with a vender laboratory to perform the same kind of DNA analysis that a commercial database would perform.[22] Then, the government uploads the resulting profile into one of the civilian sites.[23] Finally, the government uses "traditional investigative . . . methods" to follow up on any familial matches they discover.[24] This process is known more generally as "familial searching"; FGGS refers specifically to familial searching using civilian databases.[25]

State governments have conducted familial searches *without* using civilian databases since the early 2000s.[26] This has been possible because the FBI has maintained a DNA database in collaboration with state governments nationwide

---

18. *Id.*

19. 23ANDME, *supra* note 9.

20. Kolenc, *supra* note 6, at 66.

21. GEDMATCH, gedmatch.com (last visited July 31, 2021); Peter Aldhous, *A Security Breach Exposed More Than One Million DNA Profiles on A Major Genealogy Database*, BUZZFEED NEWS (July 22, 2020, 3:01 PM), https://www.buzzfeednews.com/article/peteraldhous/hackers-gedmatch-dna-privacy.

22. DEP'T OF JUST., *Department of Justice Announces Interim Policy on Emerging Method to Generate Leads for Unsolved Violent Crimes* (2019), https://www.justice.gov/opa/pr/department-justice-announces-interim-policy-emerging-method-generate-leads-unsolved-violent (last visited July 31, 2021).

23. *Id.*

24. *Id.*

25. *Combined DNA Index System*, FED. BUREAU OF INVESTIGATION *(CODIS)*, https://www.fbi.gov/services/laboratory/biometric-analysis/codis (last visited July 31, 2021).

26. *See* Richard Willing, *Suspects Get Snared by a Relative's DNA*, USA TODAY (June 7, 2005), Https://Usatoday30.Usatoday.Com/News/Nation/2005-06-07-Dna-Cover_X.Htm (describing a familial search in North Carolina in 2003).

called the Combined DNA Index System, or CODIS.[27] But the use of civilian databases has two important functional differences from the use of CODIS. First, civilian databases use a more advanced type of DNA analysis and contain more detailed DNA profiles than CODIS, making familial searches easier.[28] Second, civilian databases provide a larger and more diverse corpus of DNA profiles.[29]

The well-publicized Golden State Killer case serves as an example of FGGS in practice and its associated benefits. The Golden State Killer's homicide spree lasted from 1974 to 1986.[30] During that time, he roamed California, committing approximately forty to fifty rapes and a dozen murders.[31] For decades, the case was cold and the killer remained at large.[32] Then, in 2018, investigators uploaded his DNA profile to GEDmatch.[33] They discovered ten to twenty distant relatives of the killer, approximately third cousins.[34] Using those matches, the investigators were able to find their common ancestor with the killer and trace the lineage back to the present day.[35] They found two possible candidates, one of whom, Joseph DeAngelo, was confirmed as the killer by a fresh DNA sample.[36]

Besides the Golden State Killer, other high-profile cold cases solved by FGGS include the identification and capture of John D. Miller, who committed an infamous rape and murder in 1988,[37] and William Earl Talbott II, who committed a double murder in 1987.[38] The crimes FGGS has solved go as far back as the 1970s.[39] FGGS has been used to solve recent cases as well. In July

27. *Frequently Asked Questions on CODIS and NDIS*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited July. 31, 2021). The following states currently perform familial searching using CODIS: Arkansas, California, Colorado, Florida, Michigan, Texas, Utah, Virginia, Wisconsin and Wyoming. *Id.* By contrast, the federal government does not. *Combined DNA Index System*, *supra* note 25.

28. Natalie Ram, *Genetic Privacy After Carpenter*, 105 VA. L. REV. 1357, 1378–79 (2019).

29. Kolenc, *supra* note 6, at 66. Although CODIS contains over 19 million DNA profiles, it is limited to the profiles of convicts or arrestees, and thus represents only a fraction of the U.S. population. *CODIS-NDIS Statistics*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics.

30. Justin Jouvenal, *To Find Alleged Golden State Killer, Investigators First Found His Great-Great-Grandparents,* WASH. POST (Apr. 30, 2018, 3:22 PM), https://www.washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html.

31. Benjy Egel, *Here's the String of Crimes Tied to the East Area Rapist in Years of California Terror*, SACRAMENTO BEE, https://www.sacbee.com/news/local/crime/article209788654.html.

32. Jouvenal, *supra* note 30.

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. *How a Genealogist Helped Police Crack an Infamous 30-year-old Cold Case,* CBS NEWS (July 17, 2018, 7:35 AM), https://www.cbsnews.com/news/april-tinsley-murder-police-crack-cold-case-with-cutting-edge-genealogy.

38. Gearty, *supra* note 4.

39. *Id.*

2018, a man was arrested in Utah after FGGS pinned him as the perpetrator of a rape he committed a few months prior.[40]

In most of the recent high-profile FGGS cases, investigators conducted their familial search through GEDmatch rather than through a commercial database.[41] GEDmatch offers tools that 23andMe and Ancestry do not, including the ability to match based on only one particular segment of DNA.[42] Also, since GEDmatch contains DNA profiles from both Ancestry and 23andMe, as well as other commercial databases, it can find matches from across their respective user bases.[43] These qualities, along with GEDmatch's relatively more FGGS-friendly policy,[44] are probably why law enforcement prefers to use GEDmatch over 23andMe or Ancestry, despite GEDmatch's comparatively smaller database.

2. Current Restrictions on FGGS

The practice of FGGS, despite its novelty, is already restricted in several ways. For the federal government, FGGS is restricted by the Department of Justice's interim policy.[45] On the state side, an increasing number of states have enacted their own restrictions on familial searching, including outright bans.[46] Additionally, for both state and federal actors, FGGS is restricted by the privacy policies of civilian databases.[47]

On September 2, 2019, the Department of Justice approved an interim policy on FGGS that went into effect on November 11 of the same year.[48] The policy restricts the use of FGGS to three scenarios. First, it may be used if the government possesses a forensic DNA sample from the putative perpetrator of an unsolved violent crime.[49] Second, it may be used if the case involves the unidentified remains of a suspected homicide victim.[50] Third, it may be authorized by the prosecutor when there is a "substantial and ongoing threat to public safety or national security."[51]

---

40. Antonio Regalado, *Genetic Genealogy is Now Solving Recent Crimes, Not Just Cold Cases*, MIT TECH. REV. (July 30, 2018), https://www.technologyreview.com/f/611748/genetic-genealogy-is-now-solving-recent-crimes-not-just-cold-cases.

41. Gearty, *supra* note 4; *see also* Sarah Zhang, *how a Genealogy Website Led to the Alleged Golden State Killer*, ATLANTIC (Apr. 27, 2018, 12:45 PM), https://www.theatlantic.com/science/archive/2018/04/golden-state-killer-east-area-rapist-dna-genealogy/559070/ (investigators uploaded the Golden State Killer's DNA to Ancestry at one point during their search, but no useful lead was found).

42. Zhang, *supra* note 41.

43. *Id.*

44. *See infra* Part I.A.2.

45. DEP'T OF JUST., *supra* note 5, at 1.

46. *Combined DNA Index System*, *supra* note 25.

47. *See infra* p. 1725.

48. DEP'T OF JUST., *supra* note 5, at 1.

49. *Id.*

50. *Id.*

51. *Id.* at 5.

In these three scenarios, before the FBI or other agencies can use FGGS, they must first have failed to find a match in CODIS.[52] They are also required to consider other "reasonable scientific alternatives."[53] Only after consulting a laboratory official on such alternatives and after the prosecutor and agency agree that FGGS is a "necessary and appropriate" step, may they proceed with the FGGS process.[54]

The policy requires agencies to identify themselves as law enforcement to the civilian database and to only use databases that notify users of the possibility of law enforcement use in criminal investigations.[55] If the government needs to collect the DNA of a non-suspect, it must do so with informed consent.[56] However, if a formal request were to "compromise the integrity of the investigation," it may instead collect the DNA covertly so long as it obtains a search warrant before sending the sample to a vender laboratory.[57] A suspect should not be arrested on the sole basis of a genetic association.[58]

The policy also lays out rules for handling the DNA data itself. Such data must be treated as confidential government information.[59] When a suspect is arrested after their genetic information has been sent to a third party, the government must request all of the suspect's data be removed from the database and returned to the government.[60] If no arrest occurs, or if an arrest occurs and after a judicial order is entered, the government may then destroy all related genetic records.[61] Throughout the process, the suspect's DNA data must only be used for identification purposes and not to learn the genetic traits of the suspect.[62]

The FBI does not purport to regulate familial searching at the state level, leaving it to the states' discretion.[63] Maryland and the District of Columbia have enacted laws to prohibit all familial searching.[64] For those states that do perform

52. *Id*. (the term "reasonable scientific alternatives" is not defined in the document).

53. *Id.*

54. *Id.* at 5–6.

55. *Id.* at 6. (all of the notable civilian databases currently include such a notification in their terms of service); *see also Terms and Conditions (US),* ANCESTRY (Oct. 15, 2019), https://www.ancestry.com/cs/legal/health-terms (last visited July 31, 2021); *Terms of Service,* 23ANDME (Sept. 30, 2019), https://www.23andme.com/about/tos (last visited July 31, 2021); *Terms and Service and Privacy Policy*, GEDMATCH (Jan. 11, 2021), https://www.gedmatch.com/terms-of-service-privacy-policy (last visited July 31, 2021).

56. DEP'T OF JUST., *supra* note 5, at 6.

57. *Id.*

58. *Id.* at 7.

59. *Id.*

60. *Id.*

61. *Id.* at 8.

62. *Id.* at 4, 6–7.

63. *Combined DNA Index System*, *supra* note 25.

64. *Id.*; MD. CODE ANN., PUB. SAFETY § 2-506(d) (West 2009) (prohibiting all "person[s]" from conducting familial searching); D.C. CODE § 22-4151(b) (2009) (prohibiting familial searching using DNA collected by a state agency).

familial searching, their regulations vary.[65] Nonetheless, there are common elements among the various statutes; for example, they all have restrictions on what kinds of crimes can be investigated using familial searching.[66]

The two largest commercial databases, Ancestry and 23andMe, both oppose FGGS. Ancestry's privacy statement declares, "Ancestry does not voluntarily cooperate with law enforcement."[67] Ancestry's Terms and Conditions (US) require that any DNA submitted must be either the user's own DNA or the DNA of someone for whom the user is a legal guardian, without exception.[68] 23andMe's Terms of Service likewise require that the user submit only their own DNA or that of a dependent.[69]

Despite these assurances, it may be that commercial databases are less resistant to law enforcement activity than their policies would suggest.[70] For example, in 2019 the company FamilyTreeDNA was revealed to have been voluntarily disclosing its users' information to the FBI, despite its stated policy that it would not do so.[71] Moreover, provisions against uploading another person's DNA may be toothless because commercial databases have no means of actually preventing such a practice.[72]

GEDmatch's policy markedly differs from those of the large commercial databases. Unlike 23andMe and Ancestry, GEDmatch allows for the uploading of another person's data by law enforcement in cases of murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault, or to identify a dead body.[73] Elsewhere in its policy, GEDmatch stresses a second time that a user's data may be used in familial searching by law enforcement.[74] To be sure, a user must "opt in" to have their data be viewable by users who identify themselves as law enforcement.[75] However, GEDmatch has previously allowed Florida law enforcement, under warrant, to conduct FGGS using its entire database.[76]

---

65. *See* Nieto, *supra* note 6, at 1772.

66. *See id.* at 1776–77.

67. *Your Privacy*, ANCESTRY (Sept. 23, 2020), https://www.ancestry.com/cs/legal/privacystatement (last visited July 31, 2021).

68. ANCESTRY, *supra* note 55.

69. 23ANDME, *supra* note 55.

70. Katelyn N. Ringrose, Note, *A Cautionary Note: Genealogy Companies Need to Stop Giving Warrantless DNA Clues to Law Enforcement*, 124 PENN. STATIM 302, 325 (2019).

71. *Id.*

72. *Id.* at 324–25.

73. GEDMATCH, *supra* note 55.

74. *Id.* ("For example, some of these possible uses of [data] . . . include but are not limited to . . . familial searching by third parties . . .").

75. *Id.* Only around 260,000 of GEDmatch's 1.45 million users have opted in. Alex Wood, *DNA, Genealogy Lead to Arrest in Series of Rapes*, J. INQUIRER (June 10, 2020), https://www.journalinquirer.com/crime_and_courts/dna-genealogy-led-to-arrest-in-series-of-rapes/article_27b25296-ab2d-11ea-8b3e-472861ca42e0.html.

76. Kashmir Hill & Heather Murphy, *Your DNA Profile is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES (Dec. 30, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html.

B. *CARPENTER* AND OTHER CASE LAW

The Fourth Amendment of the Constitution guarantees against "unreasonable" searches.[77] Courts have generally interpreted "reasonable" to require a warrant,[78] and "search" as an act of the government that infringes either a property right or a person's "reasonable expectation of privacy."[79] In delineating the scope of a "reasonable expectation," courts have developed the third-party doctrine, which states that persons have no reasonable expectation of privacy in information they disclose to a third party.[80] This doctrine was recently narrowed by *Carpenter v. United States*.[81]

1. Carpenter v. United States*: Limiting the Third-Party Doctrine*

Carpenter's technical background is somewhat complex. In short, every cellular phone connects to a cellular network several times a minute.[82] Each time the phone connects, the cellular service provider records the approximate location of the device at the moment of connection.[83] The geo-location accuracy (at the time of the facts of *Carpenter*) ranged from an eighth of a square mile to four square miles.[84] The provider stores all of these location data, which are referred to as cell site location information (CSLI).[85] As a consequence, cellular service providers possess information on the location of every cell phone user, whenever they had their cell phone on their person, for as far back as they retain the records (up to five years at the time of the decision).[86] In *Carpenter*, police obtained a court order—but not a warrant—to acquire the defendant's CSLI that the provider had acquired over a period of 127 days.[87] These data were used as evidence to link the defendant to a series of robberies.[88]

The Court began by noting that the case lay at the "intersection" of two separate lines of precedent.[89] The first line of precedent (although less a line than a single case) consisted of the agreement of a five-justice majority in *United States v. Jones* that long-term GPS monitoring of a suspect's location by the

---

While the proper scope of an FGGS warrant is a difficult question itself, this Note confines itself to the question of whether FGGS can be performed *without* a warrant.

77. U.S. CONST. amend. IV.

78. *E.g.*, Mitchell v. Wisconsin, 139 S. Ct. 2525, 2534 (2019).

79. United States v. Jones, 565 U.S. 400, 405–06 (2012).

80. Carpenter v. United States, 138 S. Ct. at 2216.

81. *Id.* at 2217.

82. *Id.* at 2211.

83. *Id.*

84. *Id.* at 2218.

85. *Id.* at 2211–12.

86. *Id.* at 2218.

87. *Id.* at 2212. The order was issued under a "reasonable grounds" standard, less exacting than the "probable cause" standard required for a warrant. *Id.*

88. *Id.* at 2212–13.

89. *Id.* at 2214–15.

government constituted a search for Fourth Amendment purposes.[90] The second line of precedent was the third-party doctrine, developed in cases such as *Smith v. Maryland* and *United States v. Miller*.[91] *Miller* applied this doctrine to a person's bank records, which are retained by the bank, and *Smith* to the numbers a person dials on their home phone, which are recorded by the telephone company.[92] Because the defendant's CSLI was long-term location information like in *Jones*, but also automatically disclosed to a third party like the dialed numbers in *Smith*, existing precedent was contradictory as to whether CSLI was protected by the Fourth Amendment.[93] A clarifying decision was needed.

The Court settled this conflict by holding that *Jones* trumped the third-party doctrine.[94] First, the Court observed that CSLI fell neatly under *Jones* because it "provides an all-encompassing record of the holder's whereabouts," revealing "movements . . . and . . . associations" and "privacies of life."[95] In fact, CSLI could be—and was—used to track a person more exhaustively than a GPS device attached to a car could.[96] "A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[97] The Court also noted that CSLI was continuing to grow more accurate and that the decision must take account of the cutting edge of technological improvements.[98]

The Court then turned to the third-party doctrine, noting the doctrine was never meant to automatically and unconditionally apply whenever a defendant has shared information with a third party.[99] It observed the information that the government had collected in *Smith* and *Miller* was somewhat limited: telephone numbers, and "negotiable instruments," respectively.[100] The Court reasoned that "[t]here is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today."[101] The

90. *Id.* at 2215. In *Jones*, the Court unanimously held that attaching a tracking device to a car constituted a Fourth Amendment search. *Jones*, 565 U.S. at 404, 413. Four justices reached that result using a property-based analysis, while another four justices used a privacy-based analysis, with Justice Sotomayor endorsing both approaches. *Id.* at 404–05, 413–14, 418–19.

91. *Carpenter*, 138 S. Ct. at 2216 (citing Smith v. Maryland, 442 U.S. 735 (1979), and United States v. Miller, 425 U.S. 435 (1976)).

92. *Id.*

93. *Id.*

94. *Id.* at 2217.

95. *Id.*

96. *Id.* at 2218.

97. *Id.*

98. *Id.* at 2218–19.

99. *Id.* at 2219.

100. *Id*. at 2216.

101. *Id*. at 2219.

government's position, therefore, would not be a "straightforward application" of the third-party doctrine but a "significant extension" of it.[102]

The Court also noted that cell phone location information "is not truly 'shared' as one normally understands the term."[103] Cell phones and the services they provide are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[104] "[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up."[105]

The Court stressed that its decision was narrow, did not "disturb the application of *Smith* and *Miller*," and did not even extend to other possible kinds of CSLI, let alone other technologies.[106] It then confirmed that there was no applicable exception to the warrant requirement.[107]

2. Maryland v. King: *When is DNA Unproblematic?*

Before this Note turns to *Carpenter*'s application to FGGS, it is worthwhile to examine another potentially relevant case. The Supreme Court's most recent case dealing with DNA and privacy is *Maryland v. King*.[108] Although *King's* holding does not *directly* bear upon the issue of FGGS, it is helpful on some points.

The defendant in *King* was convicted of rape based on a DNA match.[109] When he was arrested for an unrelated crime, officers collected his DNA by swabbing the inside of his cheek.[110] When they checked the DNA against CODIS, they discovered a match with the earlier rape.[111] The defendant was subsequently charged and found guilty of the rape, and later challenged the constitutionality of the swab.[112] The Maryland state statute authorizing the swab only allowed swabs of persons in custody for a serious offense supported by probable cause.[113]

The Court held that since the swab involved an unwanted trespass on the defendant's person, the Fourth Amendment applied.[114] The Court then weighed the government's interests in performing the swabs against the privacy interest

102. *Id.*
103. *Id.* at 2220.
104. *Id.* (quoting Riley v. California, 573 U.S. 373, 384 (2014)).
105. *Id.*
106. *Id.*
107. *Id.* at 2221.
108. 569 U.S. 435 (2013).
109. *Id*. at 440.
110. *Id.*
111. *Id.*
112. *Id.*
113. *Id.* at 443.
114. *Id.* at 446.

implicated.[115] The swabs served the important governmental purpose of identifying the arrested person and formed part of the booking process.[116] In this respect, they were no different from the use of mugshots or fingerprinting.[117] The Court also noted the importance of DNA identification in absolving innocent suspects.[118]

The Court then reviewed the history of using new developments in forensic science to identify suspects and reasoned that DNA was one more step forward.[119] DNA was an even better form of identification than the last great forensic innovation—fingerprinting—because while facial features and even fingerprints can be changed, DNA typically cannot.[120]

Turning to the privacy interests, the Court held that the minimal intrusion of a cheek swab did not outweigh the immense value of DNA identification.[121] Moving on to the separate issue of the CODIS processing, the Court held that it was not unconstitutional for three reasons.[122] First, CODIS uses sections of DNA that do not reveal the genetic traits of the person from whom the DNA originates.[123] Second, the DNA in CODIS is analyzed only to generate a unique identity, not to determine genetic traits.[124] Third, the authorizing statute contained provisions against using DNA for any purpose other than identification.[125]

Ultimately, *Maryland v. King* is too narrow to be helpful in illuminating the question here.[126] This is because, unlike CODIS, the DNA samples used in civilian databases *can* be used to determine genetic traits.[127] While the opinion does mention that the statute at issue forbade familial searching, it does so only in passing.[128] The main point to take from *King* is that "a statutory or regulatory duty to avoid unwarranted disclosures' generally allays . . . privacy concerns."[129]

115. *Id.* at 447.
116. *Id.* at 451–52.
117. *Id.*
118. *Id.* at 455–56 (quoting JIM DWYER PETER NEUFELD, & BARRY SCHECK, ACTUAL INNOCENCE 245 (2000)).
119. *Id.* at 456–59.
120. *Id.* at 459.
121. *Id.* at 461.
122. *Id.* at 464.
123. *Id.*
124. *Id.*
125. *Id.* at 465.
126. Dery, *supra* note 6, at 6.
127. *See* 23ANDME, *supra* note 9.
128. Maryland v. King, 569 U.S. at 444.
129. *Id.* at 465 (quoting Nat'l Aeronautics and Space Admin. v. Nelson, 562 U.S. 134, 155 (2011)).

II. THE APPLICATION OF *CARPENTER* TO FGGS

Strictly speaking, *Carpenter* has no effect on FGGS one way or another because *Carpenter* was a narrow holding about cell site data,[130] and DNA is not cell site data.[131] But the broader rationale underlying the specific details of *Carpenter*—namely, that the third-party doctrine is limited by certain considerations—raises questions. Several commentators have considered the possible application of *Carpenter*'s rationale to FGGS, and they have routinely, if not uniformly, suggested that it should indeed apply.[132] But a closer reading of *Carpenter* reveals that DNA is not so easily analogized.

A. DISTINGUISHING *CARPENTER* DOCTRINALLY

The DNA involved in a familial search is distinguishable from CSLI in two important ways. First, users of civilian databases willingly and deliberately share their DNA, and second, DNA does not reveal a person's actions. Moreover, law enforcement does not access users' DNA information directly when it conducts FGGS.[133]

1. Users Voluntarily Share Their DNA With Civilian Databases

Since its inception, the third-party doctrine has required that the individual have *voluntarily* disclosed the disputed information to the third party.[134] In *Carpenter*, the Court noted that CSLI was not really "shared" for the purposes of the third-party doctrine for two reasons: first, because cell phones are indispensable devices in modern society; second, because a phone discloses CSLI "by dint of its operation, without any affirmative act on the part of the user."[135]

Two recent cases have expounded upon each of these prongs. In *United States v. Hood*, the defendant challenged the government's warrantless acquisition of his IP address data, arguing that *Carpenter* applied.[136] The First Circuit disagreed, noting that the defendant had generated the data "only by

130. *Carpenter*, 138 S. Ct. at 2220.

131. In his concurring opinion in *Carpenter*, Justice Gorsuch mused: "Can the government . . . secure your DNA from 23andMe without a warrant or probable cause? . . . . [T]hat result strikes most lawyers and judges today—me included—as pretty unlikely." *Id.* at 2262. However, FGGS does not directly secure other users' DNA. *See* Lindsey Van Ness, *DNA Databases Are Boon to Police but Menace to Privacy, Critics Say*, PEW: STATELINE (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 ("Schubert said police don't get behind-the-scenes, unlimited access to peruse DNA databases, despite what many people believe. Instead, investigators upload a DNA profile and get a list of matches and partial matches like the average user, she said in an interview.").

132. *See, e.g.,* Dery, *supra* note 6, at 121–28; Ringrose, *supra* note 69, at 318.

133. *See* Van Ness, *supra* note 131.

134. *Carpenter*, 138 S. Ct. at 2220.

135. *Id.*

136. United States v. Hood, 920 F.3d 87, 91 (1st Cir. 2019).

making the affirmative decision to access a website or application. By contrast . . . every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger."[137]

In *Naperville Smart Meter Awareness v. City of Naperville*, the defendant city had used "smart meters" to collect detailed energy consumption data from citizens' houses.[138] The plaintiffs challenged this practice as a violation of their Fourth Amendment rights.[139] On appeal, the defendant argued that the third-party doctrine permitted it to collect the data.[140] The Seventh Circuit applied *Carpenter*, observing that the citizens effectively had no choice but to purchase electricity from the city, just as people have little choice but to use cell phones.[141]

FGGS is distinguishable from CSLI on both prongs of this analysis. First, consider indispensability. Genetic testing is a discretionary service, not an essential one. It serves the functions of identifying predisposition to certain diseases, locating a person's relatives, and allowing a person to learn their genetic ancestry.[142] The last of these serves little more than curiosity. The others are undoubtedly useful, but they are very far from being as "indispensable to participation in modern society" as cell phones are.[143] Admittedly, technology ever advances, and it is at least possible that genetic testing will one day be as ubiquitous as cell phone usage. But that is by no means certain and does not affect the analysis of today.[144]

Second, the disclosure of genetic information to a genetic testing company is undoubtedly an "affirmative act." In *Miller*, the third-party doctrine applied to information that was merely disclosed "in the ordinary course of business."[145] But for civilian databases, genetic information *is* the business. The very premise of a commercial database is that the customer will disclose their genetic information to the company, which will then be analyzed and presented to the customer.[146] To disclose their genetic information, the customer must purchase a testing kit, deposit saliva into a tube, and mail the tube to the company's laboratory.[147] One could hardly imagine a more deliberate disclosure. In this

137. *Id.* at 92.
138. Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 524 (7th Cir. 2018).
139. *Id.*
140. *Id.* at 527.
141. *Id.*
142. *See generally* ANCESTRY, https://www.ancestry.com/dna/ (last visited July 31, 2021).
143. Kolenc, *supra* note 6, at 97–98.
144. *Id.*
145. United States v. Miller, 425 U.S. at 442.
146. 23ANDME, *supra* note 9.
147. *How Does AncestryDNA Work? An Inside Look at The Process*, ANCESTRY, https://www.ancestry.com/dna/lp/how-does-ancestrydna-work (last visited July 31, 2021). Moreover, open databases like GEDmatch require the *additional* step of downloading one's raw data from a commercial database, then uploading it to the open database. *See* GEDMATCH, *supra* note 55.

respect, civilian DNA databases fit into the third-party doctrine more neatly than even the doctrine's foundational cases.

The Court in *Carpenter* declined to overrule *Smith* and *Miller*,[148] even though those cases each involved an indispensable aspect of modern life—home telephone usage and banking, respectively—and each also involved a disclosure that was only incidental to doing business.[149] Since FGGS involves a non-essential service and a deliberate, affirmative disclosure central to a transaction, it deals with data that were shared more definitively than in *Smith* and *Miller*. *Carpenter*, then, cannot restrict FGGS on the ground that it accesses data that were not "shared." If the *Carpenter* rationale were to have any bearing on the status of FGGS, it would be on account of the nature of the data.

2. The Nature of DNA Compared with Location Information

In deciding *Carpenter*, the Court repeatedly emphasized the power of location information to divulge many intimate details of a person's life.[150] It commented that the Court in *Smith* did not foresee the "novel circumstances" of such a "detailed and comprehensive record of [a] person's movements."[151] Applying the third-party doctrine would go against "society's expectation . . . [that] law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[152] The privacy interest violated was that "in the whole of [one's] physical movements."[153]

Following *Carpenter*, the Circuit courts have recognized location information as deserving of special treatment. In *United States v. Hood*, the First Circuit held that *Carpenter* did not apply to IP address information because that information was not location information.[154] In *United States v. Beverly*, the government collected various non-CSLI data related to the defendant's phone.[155] The defendant argued that the data should be suppressed under *Carpenter* because they might be used to track his location.[156] The Fifth Circuit rejected this argument because the defendant had no basis for his claim that the data could be so used.[157] "With no showing of that," said the court, "[the defendant]'s attempt to force this evidence into *Carpenter*'s holding is a nonstarter."[158]

148. *Carpenter*, 138 S. Ct. at 2220.
149. *Miller*, 425 U.S. at 442; *Smith*, 442 U.S. at 742.
150. *Carpenter*, 138 S. Ct. at 2218.
151. *Id.* at 2217.
152. *Id.* (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring)).
153. *Id.* at 2219.
154. 920 F.3d 87, 92 (1st Cir. 2019).
155. 943 F.3d 225, 231 (5th Cir. 2019).
156. *Id.* at 233.
157. *Id.* at 235.
158. *Id.* at 239.

This granting of a special status to location information fits into a broader Fourth Amendment trend of protecting information that tends to reveal the pattern of a person's day-to-day actions. In *Riley v. California*, the data stored on a cell phone were held to be protected in part because they could "form a revealing montage of the user's life."[159] Both *Riley* and *Carpenter* quote the same line from Justice Sotomayor's concurrence in *Jones*: location data can reveal a person's "familial, political, professional, religious, and sexual associations."[160] Thus, data that reveals "associations" seems to be afforded special protection.

Some commentators have suggested that DNA can "map" a person's behavior just as CSLI can, indicating that courts should apply the *Carpenter* rationale.[161] It may be true that DNA can reveal a disposition more inclined towards particular behavior, but an inclination towards an action is not an action. DNA cannot reveal anything about a person's *actual* actions, conduct, or character.

Exactly what sorts of information *does* DNA reveal, then? 23andMe advertises that its DNA analysis can reveal some physical traits such as eye and hair color, the shape of some facial features, medical predispositions, and sensitivity to certain tastes.[162] And, of course, it can reveal the genetic relationships between people.[163] Let us examine these types of personal information one at a time.

First, there is information about a person's facial features. As personal information goes, one's facial features are as far from private as one might imagine. True, there are growing political and legal concerns about the privacy implications raised by ever-improving facial recognition technology.[164] But DNA facial reconstruction is inherently limited because facial structure is affected by factors other than DNA, such as hormonal variation, epigenetics, and cosmetic alteration.[165]

Then there is information about a person's propensity for certain diseases. This is, in most circumstances, the most private and intimate of the details that may be revealed by DNA testing. Yet even this information does not actually

159. 573 U.S. 373, 396 (2014).

160. *Id.*; *Carpenter*, 138 S. Ct. at 2217.

161. *See* Dery, *supra* note 6, at 126–28.

162. 23ANDME, *supra* note 9.

163. *Id.*

164. *See, e.g.,* Patel v. Facebook, Inc., 932 F.3d 1264, 1267 (9th Cir. 2019) (facial recognition technology caused concrete harm to plaintiffs' privacy interests).

165. Peter Claes, Denise K. Liberton, Katleen Daniels, Kerri Matthes Rosana, Ellen E. Quillen, Laurel N. Pearson, Brian McEvoy, Marc Bauchet, Arslan A. Zaidi, Wei Yao, Hua Tang, Gregory S. Barsh, Devin M. Absher, David A. Puts, Jorge Rocha, Sandra Beleza, Rinaldo W. Pereira, Gareth Baynam, Paul Suetens, Dirk Vandermeulen, Jennifer K. Wagner, James S. Boster & Mark D. Shriver, *Modeling 3D Facial Shape from DNA*, PLOS GENETICS 10(3) 1, 10 (2013). When the author received a genetic report from 23andMe, the report predicted physical and facial traits in terms of probability. Some predictions were inaccurate: the report predicted a low chance of cheek dimples, which the author in fact has.

reveal anything about the course of a person's life; a predisposition for a disease is not a guarantee.

Finally, there is information about a person's genetic relatives. This is not the same thing as information about "familial associations." People regularly have important familial relations with no direct genetic relationship, such as spouses, in-laws, step-relatives, and adoptive families.[166] Conversely, everyone has many genetic relatives whom they have never even met. Indeed, one of the main purposes of the commercial DNA services is to allow people to learn about those genetic relatives with whom they currently have *no* familial associations.[167]

Possible future improvements to DNA analysis should also be considered under a *Carpenter* analysis. Part of *Carpenter*'s rationale was that CSLI technology could only continue to improve in accuracy, making its use even more invasive into a person's privacy.[168] But no matter how much further DNA analysis progresses in the future, no matter how detailed it becomes, the substance of it will not change. Perhaps the list of physical traits identifiable from DNA will grow longer; perhaps the ability to find a person's relatives will increase in range of degrees of removal; perhaps more susceptibilities to disease will be pinpointed. But no new discovery can change the substantive differences between genetic information and location information. Even if the day comes when we can read a person's DNA as clearly as a book, there will be no chapter in that book detailing any action or event beyond the moment of that person's birth.

3. Could the Foregoing Analysis be Moot?

The entire privacy analysis in the context of FGGS could be moot for two reasons. The first reason has to do with the premise of an expectation of privacy. Thus far, this Note has discussed a person's privacy interest (or lack thereof) in their own uploaded DNA. But when a familial search is conducted, the proper question may not be "what expectation of privacy is there in your DNA?" but rather "what expectation of privacy is there in a genetic relative's DNA?"[169] The answer is probably that there is none, because there is probably no societal expectation of privacy in another person's body.[170] In fact, a would-be plaintiff may not even have standing to make the argument, for want of a legally cognizable injury.[171]

166. *See*, *e.g.*, *Remarriage in the United States*, UNITED STATES CENSUS BUREAU (Mar. 10, 2015), https://www.census.gov/library/publications/2015/acs/acs-30.html.

167. 23ANDME, *supra* note 9 ("Discover people who share your DNA. From close family members to distant ones, you'll be amazed by the way your DNA relatives connect you to the world.").

168. *Carpenter*, 138 S. Ct. at 2218–19.

169. Kolenc, *supra* note 6, at 75–77.

170. *Id.*

171. *Id.*

The second reason has to do with the premise that genetic information will be revealed to the government by FGGS. Thus far, this Note has discussed DNA privacy as if FGGS necessitated examining the whole of a person's genetic data and all the personal implications thereof. But in fact, FGGS does not involve examining every detail of a person's DNA—it only requires a determination of whether and to what extent it matches other sets of DNA.[172] Indeed, the DOJ's policy dictates that "personal genetic information [shall not be] transferred, retrieved, downloaded, or retained by [civilian database] users—including law enforcement—during the automated search and comparison process."[173] It also states that "[i]nvestigative agencies shall use biological samples and [FGGS] profiles only for law enforcement identification purposes . . . . Biological samples and FGGS profiles shall not be used by investigative agencies, vendor laboratories, [civilian databases], or others to determine the sample donor's genetic predisposition for disease or any other medical condition or psychological trait."[174]

In *King*, the Supreme Court reiterated its longstanding doctrine that "a 'statutory or regulatory duty to avoid unwarranted disclosures' generally allays . . . privacy concerns."[175] So long as a policy like the DOJ's is in place, the complex DNA data used in FGGS is no more of a tattle-tale than is the non-coding DNA in *King*. It has become a characterless identifier, like a fingerprint or an identification number.

B. DISTINGUISHING *CARPENTER* POLITICALLY

Having completed a survey of the doctrinal issues, the next step is to examine the practical implications to assess whether FGGS *ought* to be doctrinally unrestrained.

With the present surge in the online promulgation of DNA data, there are serious concerns that a lack of privacy safeguards may lead to a rise in genetic discrimination.[176] True, there is the DOJ's policy against using DNA data for any purpose but identification, coupled with the principle (invoked in *King*) that a formal duty to avoid disclosure may be sufficient.[177] However, while such safeguards may satisfy on a formalistic level, they may not prove to be so satisfying on a practical level. After all, our nation's history is replete with examples of discrimination in the face of de jure guarantees against

172. *See* Van Ness, *supra* note 131.

173. DEP'T OF JUST., *supra* note 5, at 3.

174. *Id.* at 6–7.

175. *King*, 569 U.S. at 465.

176. Drew M. Baldwin, *Redefining the Third-Party Doctrine: Carpenter's Effect on DNA Privacy*, 108 KY. L.J. 153, 171 (2019).

177. *King*, 569 U.S. at 465.

discrimination.[178] However, the risk of genetic discrimination resulting from FGGS seems to be low, if only because extrapolating medical details is not necessary to conduct FGGS. Additionally, the fact that investigators have thus far used GEDmatch, instead of databases with larger user bases and FGGS prohibitions, suggests that they are willing to respect the policies of civilian databases. To object to genetic databases because they might conceivably lead to genetic discrimination, could be compared to objecting to mugshots because they might lead to discrimination on the basis of color.

What is more, the use of FGGS may have an *anti*-discriminatory effect when it comes to race. African Americans are overrepresented in CODIS.[179] The highest-profile murderer brought to light by a familial search of CODIS, Lonnie Franklin, Jr., is black.[180] By contrast, people of Northern European ancestry are more heavily represented in civilian databases.[181] Of the murderers brought to justice in the recent wave of FGGS-based arrests, most were white.[182] Thus, FGGS may serve to ameliorate the disparate racial impact which would result from the exclusive use of CODIS.[183]

Some commentators, while conceding that FGGS is not restricted by the Fourth Amendment, have called for statutory or executive regulation of FGGS to prevent abuses that might result from a complete absence of standards.[184] Since those articles were written, the DOJ has issued its policy, fulfilling that regulatory role at the federal level and setting an example for states to follow.

Other writers have raised the possibility of false positives, noting that the Golden State Killer investigators had to approach several DNA-matching suspects before they found the culprit.[185] But those same investigators were able to clear the innocent men and confirm the only guilty one by collecting new DNA samples.[186] It is an inevitable part of criminal investigation, so long as its methods are imperfect and its conductors not omniscient, that innocent citizens

178. *See, e.g.*, South Carolina v. Katzenbach, 383 U.S. 301, 310–15 (1966) (discussing the history of voting discrimination in spite of constitutional and statutory guarantees of a right to vote).

179. Kim Zetter, *DNA Sample from Son Led to Arrest of Accused "Grim Sleeper*,*"* WIRED (July 12, 2010, 7:41 PM), https://www.wired.com/2010/07/dna-database.

180. *Id.*

181. Antonio Regalado, *A DNA Detective Has Used Genealogy to Point Police to Three More Suspected Murderers*, MIT TECH. REV. (June 26, 2018), https://www.technologyreview.com/f/611548/a-dna-detective-has-used-genealogy-to-point-police-to-three-more-suspected.

182. *Id.*

183. Christi J. Guerrini, Jill O. Robinson, Devan Petersen & Amy L. McGuire, *Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique*, PLOS BIOLOGY, Oct. 2018, at 1, 5. A survey suggests that support for FGGS among the general public does not vary significantly based on income or race. *Id.*

184. *E.g.*, Jamie M. Zeevi, *DNA is Different: An Exploration of the Current Inadequacies of Genetic Privacy Protection in Recreational DNA Databases*, 93 ST. JOHN'S L. REV. 767, 771–73 (2019).

185. Kolenc, *supra* note 6, at 54–55.

186. *Id.*

will sometimes fall under suspicion. If anything, DNA analysis, because of its accuracy, is the method *least* likely to place an innocent person under suspicion.

An example of DNA's favored status may be gleaned from a comparison of *Riley* and *King*. Both cases involved a search conducted on a person who had just been arrested, with the accompanying decrease in expectations of privacy.[187] In each case, the Court nevertheless held that a privacy interest was implicated.[188] But in *Riley*, the Court held that the cell phone data were not valuable enough to justify the intrusion, while in *King*, the defendant's DNA and its ability to act as an identifier was of great enough value to outweigh the intrusion.[189]

In *King*, the Supreme Court lauded the unparalleled power of DNA databases to reveal the guilty and spare the innocent.[190] Yet *King* dealt only with government-database, non-familial searching.[191] In the years since *King*, FGGS has made strides which make the method used in *King* seem insignificant by comparison. It has solved one of the most notorious serial murder cases in the nation's history.[192] It has pinpointed the culprits of crimes as old as thirty years before, and as recently as two months before.[193] The latter cases, in particular, inspire hope that victims in the future may not have to wait long for justice to be done, as previous generations have.

III. MOVING FORWARD: PREDICTIONS AND RECOMMENDATIONS

What lies ahead for FGGS? The commercial databases will probably continue to update their privacy policies, trying to strike a balance between assuaging their customers' fears and maximizing the extent to which they can profit from their customers' data. Perhaps they will keep to their present privacy pledges, and perhaps not. Either way, it will be of little importance for FGGS, because most or all FGGS will not be conducted through them but through GEDmatch due to that site's significant advantages.

The final version of the DOJ's policy was originally planned to be issued sometime in 2020.[194] At the time of this Note's publication, the final policy has not been released or a new date set. What changes will the final version make, and how will it be implemented in practice? Such speculation lies beyond this Note, but to the extent that the policy's provisions do not significantly deviate from those of the interim version, they will probably satisfy the requirements of Fourth Amendment law and the associated practical concerns.

187. *Riley*, 573 U.S. at 391–92; *King*, 569 U.S. at 463.
188. *Riley*, 573 U.S. at 403; *King*, 569 U.S. at 446.
189. *Riley*, 573 U.S. at 403; *King*, 569 U.S. at 465.
190. *King*, 569 U.S. at 460–61.
191. *Id.* at 441.
192. Jouvenal, *supra* note 30.
193. Regalado, *supra* note 40; CBS NEWS, *supra* note 37.
194. DEP'T OF JUST., *supra* note 22.

Putting official policy aside, it is unlikely FGGS will be used to investigate any crimes other than serious violent crimes. The time, effort, and resources FGGS can require seem to preclude such a broadened use.[195] The policies of the DOJ and GEDmatch both restrict the use of FGGS to violent crimes and a few other exigencies.[196] This comports with popular opinion: at least one study suggests that the public is much more open to the use of FGGS in violent crime cases.[197]

Concerns about genetic privacy and discrimination should not be discounted. As technology advances, the law sometimes struggles to keep up, and genetics is no exception. For example, there are gaps in the Genetic Information Nondiscrimination Act regarding discrimination on the basis of genetics that need to be statutorily addressed.[198] However, that is outside the responsibility of those who perform FGGS. Their part is to ensure they do not collect information on the more sensitive details revealed by DNA, and merely identify the similarities between DNA profiles.

Considering the potential value of FGGS, states that have banned familial searching should consider lifting their bans. States that do not currently practice familial searching should consider doing so. States that practice familial searching should ensure they have sensible regulations to satisfy *Maryland v. King*.

All three groups can look to the Department of Justice's policy as an example. In particular, there are two provisions within that policy that assuage popular concerns without compromising the effectiveness of FGGS. First, the policy's restriction of FGGS to violent crimes (and other exigencies) brings it in line with public opinion.[199] Second, its prohibition of using a suspect's DNA to learn their genetic traits is a way of averting the problem of genetic discrimination.

Although public opinion of FGGS seems to be cautiously optimistic, more could be done to educate the public on the differences between familial searching and the traditional government subpoena of data.[200] The increasing amount of governmental data surveillance is a growing concern among

195. *See* Jouvenal, *supra* note 30 (Golden State Killer FGGS required piecing together twenty-five family trees containing thousands of people, a process taking months).

196. DEP'T OF JUST., *supra* note 5, at 4–5; GEDMATCH, *supra* note 55.

197. Guerrini et al., *supra* note 183, at 3.

198. Baldwin, *supra* note 176, at 173–75.

199. Guerrini et al., *supra* note 178, at 3.

200. In a survey, only 48% of respondents approved of "DNA testing companies sharing their customers' genetic data with law enforcement agencies in order to help solve crimes." Andrew Perrin, *About Half of Americans are OK with DNA Testing Companies Sharing User Data with Law Enforcement*, PEW RESEARCH CTR.: FACT TANK (Feb. 4, 2020), https://www.pewresearch.org/fact-tank/2020/02/04/about-half-of-americans-are-ok-with-dna-testing-companies-sharing-user-data-with-law-enforcement. But FGGS does not involve the sharing of users' data. *See* Van Ness, *supra* note 131.

Americans.[201] But familial searching does not implicate the same concerns. Since it involves posing as a user, the government cannot uncover any information about a person that they have not already made available to other users. The point should also be emphasized that FGGS is no more a risk to privacy than CODIS familial searching.[202]

On the civilian side, commercial databases like 23andMe and Ancestry should consider revising their privacy policies, because familial searching does not threaten the privacy of those sites' users any more than other users do.[203] An opt-in provision, like the one used by GEDmatch, would allow these databases to contribute to FGGS while still respecting the wishes of their users. 23andMe, it should be noted, already encourages its users to volunteer their DNA data for scientific research.[204] A similar volunteer system for law enforcement purposes should not seem out of the question. Finally, the author would encourage his readers who have used 23andMe or another commercial service to consider uploading their data to an open database such as GEDmatch. Increasing the size and scope of such a database serves the public interest without disclosing any more information than you already have.

CONCLUSION

FGGS is a powerful new forensic tool that has already, in its brief existence, put many infamous criminals behind bars. It is not a "search" subject to the usual warrant requirement under the *Carpenter* decision because DNA information, unlike location information, cannot reveal anything about a person's actions or the circumstances of their life. Furthermore, there exist regulatory duties to safeguard any personal information DNA *could* reveal. Because of FGGS's extreme usefulness to society and its relative lack of privacy implications, its use should be encouraged in law and policy.

201. *E.g.*, Brooke Auxier, Lee Rainie, Monica Andersen, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CTR.: INTERNET & TECH. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information.

202. One recent survey suggested that the general public is more concerned about familial searching when it uses civilian databases than when it uses government databases. *See* James W. Hazel & Christopher Slobogin, *"A World of Difference"? Law Enforcement, Genetic Data, and the Fourth Amendment*, 70 DUKE L.J. 705, 749 (2021) (summarizing results).

203. *See supra* Part II.B.

204. *Research*, 23ANDME, https://www.23andme.com/research.

***