Duke Law Journal

VOLUME 70 JANUARY 2021 NUMBER 4

"A WORLD OF DIFFERENCE"? LAW ENFORCEMENT, GENETIC DATA, AND THE FOURTH AMENDMENT

JAMES W. HAZEL, PH.D., J.D &
CHRISTOPHER SLOBOGIN, J.D., LL.M.†

ABSTRACT

Law enforcement agencies are increasingly turning to genetic databases as a way of solving crime, either through requesting the DNA profile of an identified suspect from a database or, more commonly, by matching crime scene DNA with DNA profiles in a database in an attempt to identify a suspect or a family member of a suspect. Neither of these efforts implicates the Fourth Amendment, because the Supreme Court has held that a Fourth Amendment "search" does not occur unless police infringe "expectations of privacy society is prepared to recognize as reasonable" and has construed that phrase narrowly, without reference to society's actual views. The empirical study presented in this Article, which attempts to gauge societal privacy expectations in this terrain, suggests that laypeople consider law enforcement access to genetic information to be as intrusive as, or more intrusive than, searches of bedrooms, text messages, or emails, not only when one's DNA is held by health care providers, but also when it is

† James Hazel is a Postdoctoral Fellow at the Center for Genetic Privacy and Identity in Community Settings ("GetPreCiSe"), Vanderbilt University Medical Center ("VUMC"). Christopher Slobogin is the Milton Underwood Professor of Law at Vanderbilt University Law School.

The Authors would like to thank their colleagues at the Center for Genetic Privacy and Identity in Community Settings at VUMC for their support and constructive feedback on the manuscript. This work was sponsored by GetPreCiSe through a grant from the National Human Genome Research Institute, National Institutes of Health (#RM1HG009034).

obtained from direct-to-consumer genetic testing companies and public genealogy websites. Our research also suggests that the location of genetic information—rather than its nature, the purpose for which it is acquired, or the extent to which its surrender was voluntary—is the primary driver of these intrusiveness perceptions. Based on this research, we argue that both police access to non-governmental genetic databases and police use of covert methods to collect DNA in the hope of matching crime scene DNA require judicial authorization, although not necessarily a traditional warrant. More broadly, we argue that empirical data about the public's privacy concerns surrounding law enforcement's collection of and access to genetic data should be an integral consideration in judicial determinations of how these activities should be regulated by the Constitution.

TABLE OF CONTENTS

> *Can the government . . . secure your DNA from 23andMe without a warrant or probable cause?* Smith *and* Miller *say yes it can—at least without running afoul of* Katz*. But that result strikes most lawyers and judges today—me included—as pretty unlikely. In the years since its adoption, countless scholars, too, have come to conclude that the "third-party doctrine is not only wrong, but horribly wrong." . . . People often do reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private.*
>
> *—Justice Neil Gorsuch*[1]

INTRODUCTION

The governor of the state is brutally murdered, and the police are desperate to solve the crime.[2] They have crime scene DNA which they are very sure belongs to the perpetrator. Unable to develop any leads through traditional police work or other forensic analysis, government agents run the sample through the state DNA database of everyone who has been arrested in the state, as well as through the Combined DNA Index System ("CODIS"), the federal DNA database that

1. Carpenter v. United States, 138 S. Ct. 2206, 2262–63 (2018) (Gorsuch, J., dissenting) (quoting Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 U. MICH. L. REV. 561, 564 (2009) (footnote omitted)).

2. While this crime is hypothetical, the following actions taken by the police to solve the crime are based on real events.

contains the DNA of arrested and convicted individuals.[3] But they fail to get a match, despite the fact that CODIS alone houses over 19 million DNA profiles.[4]

The police then go to GEDmatch, a publicly accessible DNA database containing over 1 million profiles that have been generated elsewhere, submitted by people hoping to find relatives or learn more about their family trees.[5] Posing as one of those people, the police seek a match from this second source,[6] but again are unsuccessful. Police then proceed to Ancestry.com and 23andMe, commonly known as "direct-to-consumer genetic testing" ("DTC-GT") companies, which together contain over 26 million DNA profiles of consumers who have provided them with saliva or some other physical sample in the hope of finding relatives or discovering their health proclivities;[7] the agents ask both companies to see if they can come up with a match, even offering to pay for the service. The companies refuse, so the police obtain a subpoena from a judge, after she concludes that the DNA information "is relevant to an ongoing investigation."[8] The companies comply with the subpoena.[9] But, again, no match.

---

3. *CODIS-NDIS Statistics*, FED. BUREAU OF INVESTIGATION (June 2020), https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics [https://perma.cc/77FJ-TMFR].

4. *Id.*

5. Kashmir Hill & Heather Murphy, *Your DNA Profile Is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES (Dec. 30, 2019), https://nyti.ms/33lqoKi [https://perma.cc/KHY6-GNQZ]; *see also Tools for DNA and Genealogy Research*, GEDMATCH, https://www.gedmatch.com [https://perma.cc/R9RE-N8CY].

6. Tim Arango, Adam Goldman & Thomas Fuller, *To Catch a Killer: A Fake Profile on a DNA Site and a Pristine Sample*, N.Y. TIMES (Apr. 27, 2018), https://nyti.ms/2Kn641M [https://perma.cc/M9CK-HY78]; *see also* Abigail Abrams, *How Did They Catch the Golden State Killer? An Online DNA Service and His Genetic Relatives Revealed the Suspect*, TIME (Apr. 26, 2018), https://time.com/5256835 [https://perma.cc/2SP5-S4HK]; Antonio Regalado, *Hundreds of Crimes Will Soon Be Solved Using DNA Databases, Genealogist Predicts*, MIT TECH. REV. (Sept. 13, 2018), https://www.technologyreview.com/2018/09/13/140207 [https://perma.cc/WLR4-LF6U].

7. 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 [https://perma.cc/D4GM-RS9T].

8. Paul Elias, *Law Enforcement Investigators Seek Out Private DNA Databases*, AP NEWS (Mar. 26, 2016), https://apnews.com/e32f553002594ecfa5e83c160b4ba720 [https://perma.cc/EC7R-YDKJ].

9. *Id.* ("Ancestry and 23and[M]e each said they turn over customer genetic data only under court order."). *But see id.* ("23and[M]e privacy officer Kate Black . . . said that the company has never turned over genetic information despite receiving four court orders . . . [by] convinc[ing] investigators that the company's data won't help with their cases . . . .").

Finally, the police contact the administrators of the *All of Us* ("*AoU*") Research Program, a federally funded research database that contains the genetic information of hundreds of thousands of people who agreed to submit their DNA and medical records for the purpose of furthering research into genetic predispositions, especially those related to health and disease.[10] The administrators refuse access, pointing to a Certificate of Confidentiality[11] ("CoC") issued by the federal government. Police seek a court order to override the certificate and force the administrators to cooperate, based on the seriousness of the crime and the assertion that all other investigative avenues have been exhausted. But while the prosecution litigates the court order,[12] police find an easier target—a public research database created by citizen scientists that is not shielded by a CoC. Through this source, the government finally obtains a match, but it is only partial, meaning that it is the profile of a person related to the suspected perpetrator.

The police are undaunted, because this "familial matching" process leads them to four relatives of the partial match whose whereabouts at the time of the crime and other characteristics make them persons of interest. The police surreptitiously collect the DNA of three of these relatives from used coffee cups and other discarded items. Unfortunately, none is an exact match. And they are frustrated in their attempts to obtain the DNA of the fourth person, because he is extremely careful about leaving behind items that might harbor traces of his DNA. So, they subpoena his medical records and find his

10. As of May 2020, the program touted nearly 350,000 participants "and counting." Josh Denny, All of Us *Research Program Begins Beta Testing of Data Platform*, NAT'L INSTS. OF HEALTH ALL OF US RSCH. PROGRAM (May 27, 2020), https://allofus.nih.gov/news-events-and-media/announcements/all-us-research-program-begins-beta-testing-data-platform [https://perma.cc/ZCN7-7SLQ].

11. 42 U.S.C. § 241(d)(1)(E) (2018) ("Identifiable, sensitive information protected under [a Certificate] . . . shall be immune from the legal process, and shall not . . . be admissible as evidence or used for any purpose in any action, suit, or other judicial, legislative, or administrative proceeding."); *Certificates of Confidentiality (CoC) - Human Subjects*, NAT'L INSTS. OF HEALTH, https://grants.nih.gov/policy/humansubjects/coc.htm [https://perma.cc/83FB-LYKS].

12. *See* State v. Bradley, 634 S.E.2d 258, 262 (N.C. Ct. App. 2006) (recognizing a CoC holder's right to appeal from a trial court's order to disclose information protected under a CoC). CoCs have since been augmented by the 21st Century Cures Act, Pub. L. No. 114-255, 130 Stat. 1033 (2016) (codified as amended in scattered sections of 42 U.S.C.), but these new protections remain largely untested in the courts, *see* Leslie E. Wolf & Laura M. Beskow, *Genomic Databases, Subpoenas, and Certificates of Confidentiality*, 21 GENETICS IN MED. 2681, 2681 (2019) (explaining that "there is a paucity of legal cases establishing the[] effectiveness" of CoCs).

genetic profile,[13] which (finally!) is an exact match with the crime scene DNA.

Police actions like those described in this hypothetical have all happened, although not all in one case.[14] Since DNA evidence was first successfully used in a U.S. court proceeding in 1987,[15] DNA has become a powerful crime-solving tool for law enforcement, a development driven by the vast amount of genetic data now housed in government-run, public, and private databases, and the emergence of new techniques to exploit these resources. Today, not only have government-run databases containing profiles of convicted and arrested individuals expanded exponentially, but massive amounts of genetic information are also held by third parties: genetic testing has become commonplace in the health care setting; multiple large-scale precision medicine initiatives are currently underway in the United States; millions of Americans have undergone testing with DTC-GT companies; and several million more have submitted raw genetic data they have received from DTC-GT companies or elsewhere to third-party interpretation services and open-access databases seeking genealogical and other information.[16]

The genetic information housed in these public and private databases is an increasingly valuable target for law enforcement; if their contents were combined, these databases would soon—and may already—provide police with direct or familial genetic leads to

13. *See* 45 C.F.R. § 164.512(f) (2020) (authorizing certain disclosures of protected health information for "law enforcement purposes").

14. *See supra* notes 3–13. To our knowledge, *All of Us* has never subpoenaed in a criminal case, but another research-based entity has been. *See* State v. Bradley, 634 S.E.2d 258 (N.C. Ct. App. 2006).

15. Andrews v. State, 533 So. 2d 841, 843 (Fla. Dist. Ct. App. 1988) ("We have found no other appellate decision addressing the admissibility of DNA identification evidence in criminal cases."), *abrogated by* Stokes v. State, 548 So. 2d. 188 (Fla. 1989), *abrogated by In re* Amendments to the Fla. Evidence Code, 278 So. 3d 551 (Fla. 2019) (per curiam).

16. *See* Tia Moscarello, Brittney Murray, Chloe M. Reuter & Erin Demo, *Direct-to-Consumer Raw Genetic Data and Third-Party Interpretation Services: More Burden Than Bargain?*, 21 GENETICS IN MED. 539, 539 (2019) ("Up to 62% of consumers use third-party applications to interpret the raw data and health information not included in companies' reports."); Catharine Wang, Tiernan J. Cahill, Andrew Parlato, Blake Wertz, Qiankun Zhong, Tricia Norkunas Cunningham & James J. Cummings, *Consumer Use and Response to Online Third-Party Raw DNA Interpretation Services*, 6 MOLECULAR GENETICS & GENOMIC MED. 35, 36 (2018) (reporting that 67% of 478 surveyed individuals used a third-party service to interpret raw DNA information).

everyone in the United States.[17] This potential has heightened worries about government overreach during forensic investigations, but may also affect the public's willingness to undergo testing in a health care setting or to participate in research.[18] This, in turn, may exacerbate existing health disparities and stifle scientific progress, given that fear of governmental access to personal and family genetic information is likely to be most pronounced amongst populations that have been historically underrepresented in research datasets.[19]

Despite these concerns, neither the collection of genetic samples nor its analysis and use by law enforcement has been subject to significant regulation. In *Maryland v. King*,[20] the Supreme Court held that the government may collect DNA samples from arrestees using a buccal (cheek) swab, at least when the suspected crime is serious.[21] Several states have assumed that the latter limitation will soon fall by the wayside and have enacted laws that mandate collection for a number of enumerated misdemeanors as well.[22] The result is that law enforcement agencies can access their own databases containing a huge number of DNA profiles, virtually at will, as long as their purpose is to identify a suspect in a criminal investigation. And neither federal nor state law has much to say about police use of DNA collected by public

17. *See* Yaniv Erlich, Tal Shor, Itsik Pe'er & Shai Carmi, *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCI. 690, 690 (2018) ("[A] genetic database needs to cover only 2% of the target population to provide a third-cousin match to nearly any person." (citation omitted)).

18. *See* Ellen W. Clayton, Colin M. Halverson, Nila A. Sathe & Bradley A. Malin, *A Systematic Literature Review of Individuals' Perspectives on Privacy and Genetic Information in the United States*, PLOS ONE 10–11 (Oct. 31, 2018), https://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0204417&type=printable [https://perma.cc/B9TJ-7NSR] (cataloging studies indicating concern about governmental access to genetic information and noting that "worries about privacy led [some] people to decide not to participate in research").

19. *See id.* at 12–13 ("In almost all studies reporting differences in perspectives by race or ethnicity, non-White individuals had greater concerns about privacy . . . ."); *see also* Latrice G. Landry, Nadya Ali, David R. Williams, Heidi L. Rehm & Vence L. Bonham, *Lack of Diversity in Genomic Databases Is a Barrier to Translating Precision Medicine Research into Practice*, 37 HEALTH AFFS. 780, 782 (2018) (recognizing a "reasonable genetic representation of individuals of European ancestry in databases but poorer representation of other ethnic populations").

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

21. *Id.* at 456–66.

22. *See DNA Arrestee Laws*, NAT'L CONF. STATE LEGISLATURES (2013), http://www.ncsl.org/Documents/cj/ArresteeDNALaws.pdf [https://perma.cc/5HWL-FRXX] (reporting that several states collect DNA from individuals arrested for enumerated misdemeanors, including Alabama, Arizona, Kansas, Louisiana, Minnesota, North Carolina, South Carolina, and South Dakota).

and DTC-GT companies, which is regulated almost entirely by contract between the consumer and the company.[23] The Food and Drug Administration has put some limits on the types of health-related tests these companies can market,[24] and the Federal Trade Commission has issued recommended guidelines regarding their privacy policies.[25] But the statutes regulating law enforcement access to their data appear to require, at most, only a subpoena to obtain DNA.[26] Data collected for federally funded genetic research are subject to much tighter confidentiality rules, but even here a court order short of a warrant might suffice.[27]

As Justice Gorsuch suggested in the passage quoted at the beginning of this Article, however, all of this may be in flux. The elephant in the room is the Fourth Amendment, which prohibits unreasonable searches and seizures and requires a warrant based on probable cause for searches of the "persons, houses, papers, and effects" of people suspected of ordinary crime.[28] Justice Gorsuch suggests, and we agree, that this language should impose serious constraints on many types of genetic forensic investigations.[29]

Admittedly, as of right now, a significant amount of Supreme Court precedent stands in the way of those of us espousing this view. Although *King* held that a Fourth Amendment search occurs when the government collects a DNA sample from an individual,[30] it also

23. These contracts generally take the form of "a Privacy Policy (PP) or Terms of Service (ToS) document." James W. Hazel & Christopher Slobogin, *Who Knows What, and When?: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies*, 28 CORNELL J.L. & PUB. POL'Y 35, 47–57 (2018) (describing the ease with which these documents can be changed); *see also* Andelka M. Phillips, *Reading the Fine Print When Buying Your Genetic Self Online: Direct-to-Consumer Genetic Testing Terms and Conditions*, 36 NEW GENETICS & SOC'Y 273, 281–89 (2017) (describing common policy and contract provisions among DTC-GT companies).

24. Patricia J. Zettler, Jacob S. Sherkow & Henry T. Greely, *23andMe, the Food and Drug Administration, and the Future of Genetic Testing*, 174 JAMA INTERN. MED. 493, 493–94 (2014).

25. Elisa Jillson, *Selling Genetic Testing Kits? Read On*, FTC (Mar. 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/03/selling-genetic-testing-kits-read [https://perma.cc/GAZ7-WT8B].

26. *See infra* text accompanying notes 154–157 (describing HIPAA regulations permitting even medical records to be accessed with a subpoena).

27. *See* Wolf & Beskow *supra* note 12 (describing the paucity of regulation in this area).

28. U.S. CONST. amend. IV.

29. Carpenter v. United States, 138 S. Ct. 2206, 2262–63 (2018) (Gorsuch, J., dissenting)

30. Maryland v. King, 569 U.S. 435, 446 (2013) ("It can be agreed that using a buccal swab on the inner tissues of a person's cheek in order to obtain DNA samples is a search.").

concluded that if the individual is an arrestee taken into custody or a convicted individual, the search is reasonable even without a search warrant or any level of probable cause; according to the Court, these individuals have virtually no expectation of privacy in light of their incarcerated status and the minimal intrusion of a swab.[31] And if a private or public company collects DNA, the Fourth Amendment is not implicated at all, because no government action is involved.[32]

Even when the government seeks access to the DNA collected by these companies in the ways highlighted by our hypothetical, the Fourth Amendment remains irrelevant. One could argue that, in contrast to the circumstances in *King*, the DNA obtained from private companies comes from individuals whose privacy is not diminished by virtue of being incarcerated and thus that the Fourth Amendment should apply with full force. However, under the Court's current precedent, the stronger argument is that the Fourth Amendment is not implicated by such access, because the government's effort is not a "search"—a word the Supreme Court has long defined, since the 1967 decision of *Katz v. United States*,[33] in terms of whether the government action infringes an expectation of privacy "that society is prepared to recognize as 'reasonable.'"[34] Under that formulation, the Supreme Court has held that people who voluntarily surrender information to a third party, even very private information, assume the risk the third party will turn it over to the government. Thus, any expectation of privacy a party may have in the surrendered information is unreasonable, even if there is an agreement with the third party that the information will be used for a specific, non-law enforcement purpose.[35] This body of law—dubbed the "third-party doctrine"—would seem to permit warrantless police access to DNA from a third-party database.

Signs of change are in the air, however. In the past decade, the Court has significantly tempered its views on the scope of the Fourth

---

31. *See id.* 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."). *But see id.* ("This is not to suggest that any search is acceptable solely because a person is in custody.").

32. *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (establishing that only searches and seizures carried out by government officials implicate the Fourth Amendment).

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

34. *Id.* at 361 (Harlan, J., concurring).

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

Amendment. In 2012, the Supreme Court indicated it might be willing to backtrack on the third-party doctrine in a case involving real-time technological tracking,[36] and, in 2018, in *Carpenter v. United States*,[37] it explicitly did so, by holding that police need a warrant to obtain cell-site location information from a third-party carrier.[38] So, there is now room to argue that the same rule should apply to police attempts to obtain DNA from a third party, at least under some circumstances. The key question then becomes, under what circumstances, precisely?

In this Article, we argue that this question cannot be answered simply with armchair philosophizing. Rather, it requires, as the Court's case law seems to suggest, some sense of the expectations of privacy that are actually "recognized by society." One possible reference point is positive law.[39] But sole reliance on that source is problematic for a number of reasons.[40] As one of us has argued in previous scholarship, privacy is a "normative" concept in the social science meaning of that word.[41] Its scope largely depends on societal views, not on what judges might surmise from the bench or on what legislatures, driven by

36. *See* United States v. Jones, 565 U.S. 400, 404 (2012) (holding that planting a GPS device on a car is a trespass that triggers Fourth Amendment protection, even if it only tracks travel in public that is also observable by third parties).

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

38. *Id.* at 2223.

39. *See, e.g.*, *id.* at 2268, 2272 (Gorsuch, J., dissenting) ("[A]ncient principles [of bailment] may help us address modern data cases . . . ."); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1823 (2016) ("Fourth Amendment protection should depend on property law, privacy torts, consumer laws, eavesdropping and wiretapping legislation, anti-stalking statutes, and other provisions of law generally applicable to private actors . . . ."); Morgan Cloud, *A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment*, 3 OHIO STATE J. CRIM. L. 33, 72 (2005) (arguing for a Fourth Amendment "rooted in property theories").

40. *See generally* Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313 (2016) (arguing that "government action is fundamentally different — and often more deserving of regulation — than similar conduct by private parties," and thus that privacy-related measures applicable to private parties should at most establish a "floor" for Fourth Amendment protection, not a ceiling); Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment's Prohibition on Unreasonable Searches*, 48 TEX. TECH L. REV. 143 (2015) (responding to arguments that, instead of focusing on privacy, Fourth Amendment protections should protect property, dignity, intimate relationships, autonomy, and security, among other values).

41. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 113–16 (2007) ("[W]hen privacy 'is understood as a form of dignity, there can ultimately be no other measure of privacy than the social norms that actually exist in our civilization'" (quoting Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2094 (2001))).

numerous diverging agendas, might enact. Until the Court changes its Fourth Amendment focus from privacy to something else, actual societal expectations of privacy should be highly relevant to the analysis.

In an effort to find out what society thinks about the privacy interests implicated by our hypothetical (but still real-world) situation, we recruited 1,597 participants using an online survey platform and presented them with 21 short scenarios. Some scenarios involved government efforts to obtain genetic information and some described government attempts to garner other types of sensitive personal information, such as medical records, text messages, web-browsing history, and similar items. The scenarios were designed to reflect current or emerging ways in which law enforcement might try to obtain genetic and nongenetic evidence, with several based on Supreme Court precedent. Participants were asked to rank each scenario on a 100-point scale ranging from "not intrusive at all" to "extremely intrusive," and then asked to indicate whether the scenario described a situation in which a person was entitled to a "reasonable expectation of privacy." To gain a more nuanced perspective of the participants' views on privacy, we employed five variations of our survey. In the additional variations, scenarios remained largely unchanged but were presented either in the first person or with additional information or assumptions surrounding the search.

The collective goal of these surveys was to gauge public attitudes toward different types of genetic investigations, both compared to each other and compared to other types of investigations. For example, do individuals perceive law enforcement efforts to obtain genetic data from DTC-GT companies to be as intrusive as efforts to obtain the same information from their doctor? How does the perceived intrusiveness of these types of actions compare to the perceived intrusiveness of searches of bedrooms or pat downs of one's clothing during a stop and frisk? And in any of these contexts, are privacy interests perceived as diminished when people are provided additional context about the purpose of the police search—for example, to solve or prevent a serious crime—or told that the search yielded evidence of a crime?

In this Article, we attempt to obtain preliminary answers to these questions with the aim of informing debates about the appropriate level of regulation for genetic investigations, particularly as a matter of Fourth Amendment jurisprudence. Part I discusses the evolving legal

framework that governs searches involving genetic information and surveys the current and emerging ways in which law enforcement might utilize the information gleaned from such searches. Part II describes the survey methodology used in our study, the results of which are described in Part III. The Article concludes in Part IV with a discussion of the findings of the study and its implications for the Fourth Amendment third-party doctrine and genetic privacy more broadly.

There are several takeaways from our research. First, our subjects make significant distinctions among different types of genetic investigations, particularly between those using government-run databases on the one hand, and those using private databases (such as 23andMe) and public databases (such as GEDmatch) on the other. Second, even when such investigations involve obtaining DNA from a third party, our subjects often perceived them to be as intrusive as, or more intrusive than, many traditional police actions that the Supreme Court has established are Fourth Amendment searches subject to the warrant and probable cause requirements.

Third, contrary to the Court's reliance on guesses about when information is "voluntarily shared" with a third party, and contrary to much of the academic literature on how expectations of privacy should be assessed,[42] our subjects appeared to focus on the location of the information, not its provenance or content. At least when genetic data are the target, its location—for example, whether it is in an electronic medical record in a doctor's computer, a public database, or a government-run database—is the primary determinant of privacy expectations. That conclusion has interesting implications for the application of Fourth Amendment doctrine to investigations involving genetic information, at least to the extent that the doctrine is based on expectations of privacy that society is prepared to accept as reasonable. Specifically, it would support an argument in favor of judicial authorization both when police access nongovernmental genetic databases and when police collect DNA from individuals who have not yet been arrested. But the type of authorization might vary significantly, depending on the locus of the DNA.

42. See Slobogin, *supra* note 40, at 151–57, for an overview of the scholarship.

I. THE FOURTH AMENDMENT AND GENETIC DATA

The Supreme Court is reconsidering its Fourth Amendment jurisprudence, but the end result of this rethinking remains unclear. After briefly canvassing this jurisprudence, we describe current and emerging genetic investigation techniques and the potential impact of the Fourth Amendment on their use.

A. A Primer on Fourth Amendment Doctrine

The Fourth Amendment establishes "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[43] Thus, the amendment applies only to government actions that rise to the level of a "search," and even then, protects only against searches that are "unreasonable." Both of these concepts have been the subject of extensive legal analysis and discussion. This Article focuses on the fact that, in defining the threshold issue of when a Fourth Amendment search occurs, the Supreme Court has relied heavily on whether the police action in question infringes expectations of privacy "that society is prepared to recognize as reasonable,"[44] a standard that has been operationalized principally through the "knowing exposure doctrine" and the "third-party doctrine."

1. *The Knowing Exposure Doctrine.* In applying the reasonable expectation of privacy formulation, the Court has tended to conclude that one cannot expect privacy vis-à-vis the government if one cannot expect privacy vis-à-vis strangers. For instance, activities that take place in public or that can be observed from a public place are typically not protected by the Fourth Amendment. Thus, travels on public thoroughfares,[45] garbage placed at curbside,[46] and activities that take place in open fields beyond the home's curtilage,[47] are all subject to police examination without any Fourth Amendment restrictions, as are

43. U.S. CONST. amend. IV.

44. The most recent citation to this language comes from *Carpenter v. United States*, 138 S. Ct. 2206, 2213 (2018), although the Court has referred to this formulation in well over a dozen other cases. *See, e.g.*, Bond v. United States, 529 U.S. 334, 338 (2000) ("Our Fourth Amendment analysis . . . inquire[s] whether the individual's expectation of privacy is 'one that society is prepared to recognize as reasonable.'" (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979))).

45. United States v. Knotts, 460 U.S. 276, 285 (1983).

46. California v. Greenwood, 486 U.S. 35, 40 (1988).

47. Oliver v. United States, 466 U.S. 170, 181 (1984).

activities in the home that can be seen with the naked eye or using technology that is in "general public use."[48] Presumably, the Court would reach the same result when the police acquire a person's DNA from items discarded in public places; certainly, lower courts have done so.[49]

There are signs that the Court is reconsidering this "knowing exposure" doctrine, however. In *United States v. Jones*,[50] the Court held that tracking a car for twenty-eight days using a GPS attached to its bumper was a search, even though the GPS only tracked the car when it traveled public thoroughfares.[51] At the same time, *Jones* was limited to situations where the tracking was effected with a trespass—in this case, the attachment of the GPS device to the car.[52] More importantly, for purposes of this Article, *Jones* and its progeny did not directly confront any of the Court's precedent establishing its closely related, but still distinct, doctrine dealing with police access to information surrendered to third parties. Any discussion of the Fourth Amendment's application to police access of genetic information must confront the implications of that precedent—precedent that also may be evolving.

2. *The Third-Party Doctrine and* Carpenter. Closely related to the knowing exposure doctrine is the third-party doctrine, which severely limits Fourth Amendment protection of information handed over to third parties. Building on cases holding that undercover activity is not a search because the target "assumes the risk" that acquaintances are

48. Kyllo v. United States, 533 U.S. 27, 34 (2001).

49. *See* Elizabeth E. Joh, *DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing*, 91 B.U. L. REV. 665, 696–97 (2011) (describing a trend among lower courts to rely on *California v. Greenwood* in finding no Fourth Amendment protections for discarded DNA); *see, e.g.*, Commonwealth v. Bly, 862 N.E.2d 341, 356–57 (Mass. 2007) (DNA from cigarette butts and water bottle); State v. Athan, 158 P.3d 27, 38 (Wash. 2007) (en banc) (DNA from an envelope); State v. Wickline, 440 N.W.2d 249, 253 (Neb. 1989) (DNA from cigarette butts).

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

51. *Id.* at 404.

52. *Id.* at 404–05 (basing the decision on the fact that "[t]he Government physically occupied private property for the purpose of obtaining information"). However, five Justices would have based the decision on the ground that Jones's expectations of privacy were violated by the tracking. *See id.* at 414–15 (Sotomayor, J., concurring); *id.* at 427–28 (Alito, J., concurring) (joined by Justices Ginsburg, Breyer, and Kagan).

or will be government informers,[53] in *United States v. Miller*,[54] the Supreme Court held that individuals are not entitled to a reasonable expectation of privacy in voluntarily surrendered information even when the third party is a bank rather than an acquaintance.[55] The Court concluded that a bank depositor

> takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[56]

This third-party doctrine was applied again three years later in *Smith v. Maryland*[57] to uphold the warrantless seizure from the defendant's phone company of a number he had called, on the theory that he "assumed the risk that the company would reveal to police the numbers he dialed."[58]

Lower courts have extended this reasoning to uphold warrantless government access to records from auditors and accountants, trustees in bankruptcy, government institutions and, most importantly for our purposes, medical institutions.[59] Many commentators have harshly criticized these cases on the ground that they ignore the assumptions about privacy that most people have in these situations.[60] But until they are overturned, these cases would seem to allow law enforcement to

---

53. Hoffa v. United States, 385 U.S. 293, 303 (1966) ("The risk of being . . . betrayed by an informer or deceived as to the identity of one with whom one deals is . . . the kind of risk we necessarily assume whenever we speak." (quoting Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting))); *see also* Lewis v. United States, 385 U.S 206, 206–07 (1966) (holding that selling drugs to an undercover federal narcotics agent in the defendant's home did not constitute a search).

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

55. *Id.* at 437.

56. *Id.* at 443.

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

58. *Id.* at 744.

59. *See* SLOBOGIN, *supra* note 41, at 153 (citing cases).

60. *See, e.g.*, Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 999–1005 (2007); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1248–50 (2009); Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1375–91 (2019); 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, 2554–83 (2019).

obtain, without any Fourth Amendment impediments, DNA voluntarily submitted to a third party.

Then, in 2018, came *Carpenter v. United States*.[61] There, the Court held that law enforcement must generally obtain a warrant to gain access to cell-site location records held by the defendant's phone company.[62] The government argued that the third-party doctrine applied because the defendant "voluntarily" surrendered his location information to the company when he purchased the phone.[63] Gesturing toward the knowing-exposure doctrine, the government also contended that the location data only revealed travels in public and was not the defendant's property.[64] But 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."[65] It also emphasized that one does not "truly 'share[]'" one's location data with one's phone company, given the necessity of having a phone in modern society.[66] While the majority denied that it was upending the third-party doctrine, the dissenters contended that the decision lays the groundwork for doing precisely that.[67]

In the wake of *Carpenter*, considerable uncertainty exists about the applicability of the third-party doctrine to genetic information, even at the Supreme Court level. Justice Gorsuch, writing in dissent in *Carpenter*, expressed skepticism about the third-party doctrine generally, and specifically its application to certain categories of sensitive information such as genetic data. As the opening quote to this Article indicated, Justice Gorsuch used DNA access as an example of the proposition that "[p]eople often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private."[68]

---

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

62. *Id.* at 2217.

63. *Id.* at 2219.

64. *Id.* at 2218–19.

65. *Id.* at 2219.

66. *Id.* at 2220.

67. *Id.* at 2234 (Kennedy, J., dissenting) ("[B]y invalidating the Government's use of court-approved compulsory process in this case, the Court calls into question the subpoena practices of federal and state grand juries, legislatures, and other investigative bodies . . . .").

68. *Id.* at 2263 (Gorsuch, J., dissenting).

It remains to be seen what implications *Carpenter* will have for genetic data that has been surrendered to a third-party database. Before we provide our answer to that question, and the data that back it up, we provide an overview of the current and emerging ways in which law enforcement might utilize genetic information and discuss in greater detail the evolving legal frameworks that govern such searches.

B. Law Enforcement Use of Genetic Data

The two principal ways law enforcement agencies use genetic data are to track down potential perpetrators of crime by matching DNA found at a crime scene with the DNA of an identifiable person, and to identify human remains.[69] In a narrow set of cases, genetic information may also be useful means to discover a person's health history,[70] or to provide law enforcement with clues about the physical appearance of the perpetrator;[71] in the future, it may also help to determine the propensities of an individual for sentencing purposes.[72] While these latter types of genetic sleuthing have even greater implications for privacy and autonomy than DNA matching, today they are rare or are only beginning to be investigated. This Article focuses solely on the extent to which law enforcement uses genetic data for matching purposes—the most prolific reason by far the government wants DNA profiles.

This Section begins with a description of government-run forensic databases and law enforcement access to the data contained therein. It then discusses developments with respect to law enforcement access to genetic data maintained by third parties in public genealogy resources

---

69. *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 [https://perma.cc/JA36-7Q57].

70. For example, genetic information can be used to, inter alia, diagnose whether an individual has a disease, is a carrier for a disease, or is predisposed to a disease. *What Are the Types of Genetic Tests?*, NAT'L INSTS. OF HEALTH (Aug. 17, 2020), https://ghr.nlm.nih.gov/primer/testing/uses [https://perma.cc/7YNK-DCNT]. In a small subset of cases, this type of health-related information may provide investigative leads.

71. For example, Parabon Nanolabs markets a "Snapshot DNA Phenotyping Service" that uses crime scene DNA samples to make predictions about the physical appearance of the suspected perpetrator. *The Snapshot DNA Phenotyping Service*, PARABON NANOLABS, https://snapshot.parabon-nanolabs.com/phenotyping [https://perma.cc/PN35-UU5J].

72. Sally McSwiggan, Bernice Elger & Paul S. Appelbaum, *The Forensic Use of Behavioral Genetics in Criminal Proceedings: Case of the MAOA-L Genotype*, 50 INT'L J.L. & PSYCHIATRY 17, 21–22 (2017).

and private databases—specifically, DTC-GT companies, health care providers, and researchers. It concludes with a brief discussion of surreptitious collection and analysis of genetic material by law enforcement.

1. *Government-Run Forensic Databases.* *Maryland v. King*, decided in 2013, cleared the way for government-run databases when it held that DNA collection from arrestees "is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment."[73] But well before *King* sanctioned them on constitutional grounds, these databases had been expanding at the federal, state, and local levels.[74] Since 1994, the U.S. Department of Justice ("DOJ") has maintained a nationwide database—CODIS—consisting of federal ("NDIS"), state ("SDIS"), and local ("LDIS") levels.[75] Today, the federal government, all fifty states, and the District of Columbia contribute profiles to CODIS, which contains the genetic profiles of more than 18 million individuals who have been either arrested for or convicted of a crime, as well as over 1 million forensic profiles derived from crime scenes.[76] It has produced hits that have assisted in over five hundred thousand investigations.[77]

While the Fourth Amendment imposes few constraints on these systems, statutes do regulate their use. The DNA Identification Act of 1994[78] imposes standards, proficiency testing, and accreditation requirements on participating forensic laboratories,[79] sets privacy protection standards for data within the system,[80] and imposes steep

73. Maryland v. King, 569 U.S. 435, 466 (2013).

74. Mark A. Rothstein & Meghan K. Talbott, *The Expanding Use of DNA in Law Enforcement: What Role for Privacy?*, 34.2 J.L. MED. & ETHICS 153, 153–55 (2006).

75. OFF. OF THE INSPECTOR GEN., DEP'T OF JUST., AUDIT REPORT: THE COMBINED DNA INDEX SYSTEM ii, 4 (2001), https://oig.justice.gov/reports/FBI/a0126/final.pdf [https://perma.cc/N5SL-LEZD]; *see also Combined DNA Index System (CODIS)*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis [https://perma.cc/K953-MYGQ].

76. *CODIS-NDIS Statistics*, *supra* note 3.

77. *Id.*

78. DNA Identification Act of 1994, Pub. L. No. 103-322, 108 Stat. 2065 (codified as amended in scattered sections of 34 U.S.C. and 42 U.S.C.).

79. 34 U.S.C. §§ 12592(b), 12593(a) (2018).

80. § 12593(b).

penalties for misuse or unauthorized access.[81] All fifty states as well as the federal government have also enacted laws that regulate the compelled collection of DNA from individuals convicted of certain crimes, the results of which are then uploaded into CODIS.[82] In addition, at least thirty-one states and the federal government have authorized the preconviction collection of DNA from individuals arrested or charged with certain crimes[83]—generally felonies, but also enumerated misdemeanors in some jurisdictions.[84] Some of these new state and local databases may contain profiles that are ineligible for upload to CODIS,[85] and some may operate under less stringent laboratory standards and proficiency requirements than, or lack the privacy protections of, the national system.[86] Yet they are still routinely used in the investigatory process.[87]

An important development in this respect is the familial matching procedure alluded to in the opening hypothetical. Investigators can now use CODIS to carry out "familial DNA searching" ("FDS"), a *deliberate* search for partial matches with a DNA sample's genetic profile in order to locate possible relatives (generally following an unsuccessful attempt to obtain a direct match and often with the use of specialized, non-CODIS software).[88] Such searches are usually carried out at the SDIS level of CODIS, leaving "[e]ach jurisdiction [to] determine whether or not they are authorized to perform familial searching, and if so, the criteria and procedures governing their use of this searching process."[89] According to a 2017 survey of forensic crime laboratories, at least eleven states conduct familial DNA searching,

---

81. § 12593(c).

82. *DNA Sample Collection from Arrestees*, NAT'L INST. JUST. (Dec. 6, 2012), https://nij.ojp.gov/topics/articles/dna-sample-collection-arrestees [https://perma.cc/4SQT-2F4F].

83. *Id.*

84. *See DNA Arrestee Laws*, *supra* note 22.

85. Stephen Mercer & Jessica Gabel, *Shadow Dwellers: The Underregulated World of State and Local DNA Databases*, 69 N.Y.U. ANN. SURV. AM. L. 639, 648–49, 667–80 (2014).

86. *Id.* at 643–63.

87. *Id.* at 669.

88. *See* Sara Debus-Sherrill & Michael B. Field, *Familial DNA Searching – An Emerging Forensic Investigative Tool*, 59 SCI. & JUST. 20, 20, 23–24 (2019).

89. *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 [https://perma.cc/GGH3-HTK8]; *see* Comments on the Interim Rule, DNA Sample Collection From Federal Offenders Under the Justice for All Act of 2004 and on the Proposed Rule, DNA-Sample Collection Under the DNA Fingerprint Act of 2005 and the Adam Walsh Child Protection and Safety Act of 2006, 73 Fed. Reg. 74,936, 74,938 (Dec. 10, 2008).

and twenty-four states pursue partial matches that may be indicative of familial relationships.[90] Other jurisdictions place restrictions on FDS (for example, California[91]) or have banned this particular version of DNA searching (Maryland[92] and Washington D.C.[93] are two examples).

Legal scholars have raised numerous questions about FDS.[94] In addition to the potential for error that is associated with any attempt to match profiles, there is the high probability that innocent relatives of the "lead"—the person whose DNA is matched—will be subjected to heightened police scrutiny, including attempts to obtain their DNA in the manner described in our introductory hypothetical.[95] These relatives may never have met or even know about either the lead or the suspect, or may know about them and have tried to avoid association; in either case, FDS can disrupt or complicate family connections.[96] Furthermore, because people of color tend to be overrepresented in government-run databases, FDS using existing forensic databases can give rise, at the least, to the appearance of bias.[97] Yet, as Professor Erin Murphy has ably demonstrated, constructing either Fourth

90. SARA DEBUS-SHERRILL & MICHAEL B. FIELD, ICF, UNDERSTANDING FAMILIAL DNA SEARCHING: POLICIES, PROCEDURES, AND POTENTIAL IMPACT 11–12 (2017), https://www.ncjrs.gov/pdffiles1/nij/grants/251043.pdf [https://perma.cc/6T95-BU2A].

91. *BFS DNA Frequently Asked Questions*, CAL. DEP'T JUST., https://oag.ca.gov/bfs/prop69/faqs [https://perma.cc/N73W-NLF4] (describing California's policy to perform familial searches only on "database profiles from samples collected from convicted offenders"); *see also* Memorandum of Understanding: Familial Searching Protocol from Cal. Dep't of Just. 1–3 (June 14, 2011), https://oag.ca.gov/sites/all/files/agweb/pdfs/bfs/fsc-mou-06142011.pdf [https://perma.cc/A6EY-APTC] (listing prerequisites and conditions for conducting a familial search).

92. MD. CODE ANN., PUB. SAFETY § 2-506(d) (LexisNexis 2018) (proscribing familial searches "of the statewide DNA data base").

93. D.C. CODE § 22-4151(b) (2013) (banning familial searches of any "DNA collected by an agency of the District of Columbia").

94. *See, e.g.*, Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 330–40 (2010) [hereinafter Murphy, *Relative Doubt*] (noting multiple potential constitutional challenges against FDS); Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 STAN. L. REV. 751, 783–807 (2011) (arguing that "fortuitous" partial matching, arising from low-stringency searches for direct matches is no better than the "deliberate" partial matching of FDS); *see also* Abrahamson, *supra* note 60, at 2553–88 (viewing familial searches through the lens of the third-party doctrine).

95. Murphy, *Relative Doubt*, *supra* note 94, at 313–14.

96. *See id.* at 314 ("[E]ven mere suspicion, quickly dispelled, has the potential to disrupt a career, destroy a marriage, or ruin a life.").

97. Erin Murphy & Jun H. Tong, *The Racial Composition of Forensic DNA Databases*, 108 CALIF. L. REV. (forthcoming 2020) (manuscript at 45–46), https://ssrn.com/abstract=3477974 [https://perma.cc/N4MP-BP25].

Amendment or Equal Protection Clause arguments against FDS is difficult.[98] To date, the courts have given government-run databases and FDS a very wide berth.[99]

In the meantime, government-run forensic databases are likely to continue to grow, especially with the implementation of technologies like "RapidDNA" and portable devices that have made DNA analysis exponentially easier.[100] In 2017, President Trump signed into law the Rapid DNA Act, which amended the DNA Identification Act of 1994[101] and laid the groundwork for "police agencies to develop DNA profiles independent of crime laboratories, eliminating the need for expertise and the long turnaround time for profiling offenders for the database."[102] A number of jurisdictions have already taken advantage of this authorization.[103]

2. *Publicly Accessible Databases.* Government-run databases have tremendous crime-solving potential, but law enforcement is increasingly turning to public and private sources of genetic information for a number of reasons. First, as just noted, government-run databases tend to be heavily skewed toward low-income and non-white individuals.[104] Thus, they were useless in tracking down Joseph DeAngelo, the infamous "Golden State Killer" ("GSK") a white, middle-class ex-police officer now convicted of murdering and raping

98. Murphy, *Relative Doubt*, *supra* note 94, at 330–40. One significant problem is standing; even if the Fourth Amendment were held to apply to genetic searches, if a defendant is discovered through familial matching, only the family member in the database would generally have standing to exclude evidence. This is a remedy the innocent family member would not need. *Id.* at 334. However, the family member could seek damages and might well do so if the privacy invasion or associated stigma is significant. *See id.* at 314.

99. *See* Ram, *supra* note 94, at 790 n.191, 791 n.192 (surveying lower court decisions upholding forensic databases); *see also* United States v. Weikert, 504 F.3d 1, 8–9 (1st Cir. 2007) (surveying case law analyzing the constitutionality of the DNA Identification Act); United States v. Kincade, 379 F.3d 813, 839 (9th Cir. 2004) (en banc) ("[C]ompulsory DNA profiling of qualified federal offenders is reasonable under the totality of the circumstances.").

100. *RapidDNA*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/rapid-dna [https://perma.cc/8LXL-7T8G].

101. Rapid DNA Act of 2017, Pub. L. No. 115-50, 131 Stat. 1001 (codified at 34 U.S.C. §§ 12591, 12592, 40702, 40703).

102. Nancy Zhang, *Rapid DNA Act of 2017 (Public Law 115-50)*, SCIPOL, https://scipol.duke.edu/track/public-law-115-50-rapid-dna-act-2017/rapid-dna-act-2017-public-law-115-50 [https://perma.cc/9LSL-E7MK].

103. Heather Murphy, *Coming Soon to a Police Station Near You: The DNA 'Magic Box*,' N.Y. TIMES (Jan. 21, 2019), https://nyti.ms/2HpdDrD [https://perma.cc/4V43-CUPF].

104. Murphy & Tong, *supra* note 97 (manuscript at 45).

dozens of individuals during the 1970s and 1980s.[105] DeAngelo was discovered through a DNA search, but not one using a government database.[106] Rather, after years of dead ends, in 2018 police finally obtained a hit using a publicly accessible genealogy database, GEDmatch,[107] and a modernized version of FDS called "investigative (or forensic) genetic genealogy" or "long-range familial searching."[108]

GEDmatch allows individuals to upload existing genetic information about themselves—most commonly the raw data they received from a DTC-GT company for ancestry purposes—which can then be used for genealogy research and to locate biological relatives.[109] As the GSK case illustrates, genealogy databases like GEDmatch provide law enforcement with a complementary resource to supplement government-run forensic databases. Compared to the general population, DTC-GT users tend to be predominately of European descent, more educated, and of higher socioeconomic status.[110]

The advantages of forensic genetic genealogy that relies on a public resource such as GEDmatch extend beyond the racial makeup of the database. Unlike CODIS, which focuses on a limited set of twenty loci, profiles uploaded to GEDmatch generally consist of hundreds of thousands of single nucleotide polymorphisms ("SNPs").[111] All of this additional genetic information dramatically

105. *See* Heather Murphy & Tim Arango, *Joseph DeAngelo Pleads Guilty in Golden State Killer Cases*, N.Y. TIMES (June 29, 2020), https://nyti.ms/31zkBCy [https://perma.cc/74TF-XK78] ("DeAngelo had eluded the authorities for four decades before he was arrested in 2018 in a Sacramento suburb.").

106. *Id.*

107. Thomas Fuller, *How a Genealogy Site Led to the Front Door of the Golden State Killer Suspect*, N.Y. TIMES (Apr. 26, 2018), https://nyti.ms/2FkaItN [https://perma.cc/ZQU8-C3LD]; *Tools for DNA and Genealogy Research*, *supra* note 5.

108. Teneille R. Brown, *Why We Fear Genetic Informants: Using Genetic Genealogy To Catch Serial Killers*, 21 COLUM. SCI. & TECH. L. REV. 114, 128–29 (2020); *see* Ellen M. Greytak, CeCe Moore & Steven L. Armentrout, *Genetic Genealogy for Cold Case and Active Investigations*, 299 FORENSIC SCI. INT. 103, 103–05 (2019) (providing an overview of the science and methodology underlying the technique).

109. Charlie Osbourne, *GEDmatch Highlights Security Concerns of DNA Comparison Websites*, ZDNET (Oct. 31, 2019, 1:02 PM), https://zd.net/2BYuT1p [https://perma.cc/8HTF-V4W8].

110. J. Scott Roberts, Michele C. Gornick, Deanna Alexis Carere, Wendy R. Uhlmann, Mack T. Ruffin & Robert C. Green, *Direct-to-Consumer Genetic Testing: User Motivations, Decision Making, and Perceived Utility of Results*, 20 PUB. HEALTH GENOMICS 36, 39–42 (2017).

111. *See* Greytak et al., *supra* note 108, at 103, 106.

improves the ability of consumers, including law enforcement, to identify distant relatives and provides investigators with more insight about the degree of relatedness—for example, whether the partial match is a parent, a sibling, or a cousin of the alleged perpetrator.[112]

The police in the GSK case had to pose as the donor of the DNA they submitted,[113] given GEDmatch's policy at the time that individuals should "provide real names for registration and data upload."[114] However, in the wake of that case, GEDmatch quickly changed its policy to explicitly allow for law enforcement matching in homicide, sexual assault, and missing persons cases.[115] The service has since been used by law enforcement in at least one hundred cold cases,[116] generating dozens of leads, numerous arrests, and at least one conviction.[117] The power of long-range familial searching was dramatically illustrated by the authors of a 2019 study, who calculated that, in theory, GEDmatch could be used to identify well over half of the people in the United States who are of European ancestry, either directly or through a relative who had contributed genetic information to the database.[118] The authors predicted that this figure would rise to over 99 percent as the size of the database grew.[119]

Shortly after this study was published, however, press accounts revealed that the founder of GEDmatch had allowed the service to be

---

112. *See id.* at 103–06.

113. Arango, Goldman & Fuller, *supra* note 6.

114. *GEDmatch.Com Terms and Policy Statement*, GEDMATCH (Aug. 18, 2017), https://web.archive.org/web/20180427152614/https://www.gedmatch.com/policy.php [https://perma.cc/S4AQ-W4CB].

115. *See GEDmatch.Com Terms of Service and Privacy Policy*, GEDMATCH (May 20, 2018), https://web.archive.org/web/20180524135016/https://www.gedmatch.com/tos.htm [https://perma.cc/7EXY-ZJDG]; Debbie Kennett, *Updates to the Terms of Service and Privacy Policy at GEDmatch*, CRUWYS NEWS (May 21, 2018, 4:29 PM), https://cruwys.blogspot.com/2018/05/updates-to-terms-of-service-and-privacy.html [https://perma.cc/R8WK-Z4YL] (summarizing the changes to GEDmatch's privacy policy that occurred in the wake of the Golden State Killer revelations).

116. Peter Aldhous, *DNA Data from 100 Crime Scenes Has Been Uploaded to a Genealogy Website — Just Like the Golden State Killer*, BUZZFEED NEWS (May 17, 2018, 2:26 PM), https://www.buzzfeednews.com/article/peteraldhous/parabon-genetic-genealogy-cold-cases [https://perma.cc/D5S3-WYR2].

117. *See, e.g.*, Greytak et al., *supra* note 108, at 104; Heather Murphy, *Genealogy Sites Have Helped Identify Suspects. Now They've Helped Convict One.*, N.Y. TIMES (July 1, 2019), https://nyti.ms/2KT4k42 [https://perma.cc/92VG-MNLN].

118. *See* Erlich et al., *supra* note 17, at 690 ("[N]early 60% of long-range familial searches return . . . [results] usually correspond[ing] to a third cousin or closer relative.").

119. *Id.*

used to solve an assault case in Utah. Although the assault was brutal, it was not sexual in nature and did not result in death, so the authorization was contrary to the company's posted terms and conditions.[120] Because of the resulting public backlash, GEDmatch subsequently modified its policies to require both current and future users to opt in before their genetic information could be queried for law enforcement purposes.[121] Despite recent studies that indicate a high level of public support for the use of public databases by law enforcement to investigate serious violent crimes,[122] only a small percentage of GEDmatch users appear to have subsequently opted back in for law enforcement matching.[123] This development has vastly reduced the amount of genetic information available to law enforcement and resulted in a "sharp drop in the usefulness" of the resource, with law enforcement officials lamenting that "[t]here are cases that won't get solved or will take longer to solve."[124]

Yet GEDmatch will likely remain an important law enforcement tool and a central figure in the ongoing debate about the appropriate use of forensic genetic genealogy. In December of 2019, GEDmatch was acquired by Verogen, a forensic genomics firm that caters to law

120. *See* Peter Aldhous, *This Genealogy Database Helped Solve Dozens of Crimes. But Its New Privacy Rules Will Restrict Access by Cops.*, BUZZFEED NEWS (May 19, 2019, 3:41 PM), https://www.buzzfeednews.com/article/peteraldhous/this-genealogy-database-helped-solve-dozens-of-crimes-but [https://perma.cc/DLU4-H9NU]; Jon Schuppe, *Police Were Cracking Cold Cases with a DNA Website. Then the Fine Print Changed.*, NBC NEWS (Oct. 25, 2019, 9:53 AM), https://www.nbcnews.com/news/us-news/police-were-cracking-cold-cases-dna-website-then-fine-print-n1070901 [https://perma.cc/PFE6-YHR3].

121. Schuppe, *supra* note 120.

122. 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. 2, 2018, at 4 fig.1, https://journals.plos.org/plosbiology/article/file?id=10.1371/journal.pbio.2006906&type=printable [https://perma.cc/9AY3-MX7W] (finding that 91 percent of respondents supported the use of genealogy websites to investigate violent crimes and missing persons cases, with support dropping to just 46 percent for nonviolent crimes); *see also* Maurice Gleeson, *How Do You Feel About Your DNA Being Used by the Police? - The Results of a Survey*, DNA & FAM. TREE RSCH. (Nov. 14, 2018, 7:16 PM), https://dnaandfamilytreeresearch.blogspot.com/2018/11/how-do-you-feel-about-your-dna-being.html [https://perma.cc/F7RQ-MMQ8] (reporting that 85 percent of 639 surveyed genealogists were "reasonably comfortable" with police use of a public genealogy database containing their own DNA data "to help identify serial rapists and serial killers").

123. *See* Schuppe, *supra* note 120.

124. *Id.*

enforcement.[125] To date, the company has publicly committed to respecting the preferences of existing users regarding law enforcement matching and has vowed to resist broad warrants.[126] However, as noted previously, company policies are subject to change at any time.[127] And if, as in the past, police officers are willing to pretend the DNA they submit is theirs—or are able to obtain, as they did in one recent case, a warrant granting access to the information of all users, including those who have opted out of law enforcement searches[128]—the entire database could be at their disposal. Further, as recounted in more detail below, genealogy databases like GEDmatch are not the only nongovernmental resource that police might use to conduct long-range familial searches.

3. *Direct-to-Consumer Genetic Testing Companies.* Genetic information housed in the databases of DTC-GT companies represents an increasingly valuable target for law enforcement. More than 26 million individuals have now undergone testing with such companies, which today exist in the hundreds.[129] These companies offer services that purport to translate a person's genetic information into insights about their health, ancestry and family relationships, lifestyle choices, and a host of other areas.[130] The amount of genetic information

125. Megan Molteni, *A DNA Firm That Caters to Police Just Bought a Genealogy Site*, WIRED (Dec. 9, 2019, 9:01 PM), https://www.wired.com/story/a-dna-firm-that-caters-to-police-just-bought-a-genealogy-site [https://perma.cc/9QGS-BS8U].

126. *Id.*

127. Hazel & Slobogin, *supra* note 23, at 49. Further, DTC-GT databases may experience security breaches with implications for law enforcement matching that can undermine a company's stated policies. On July 19, 2020, GEDmatch experienced "a security breach orchestrated through a sophisticated attack . . . [and] [a]s a result . . . all user permissions were reset, making all profiles visible to all users." *GEDmatch Incident Response*, VEROGEN (July 20, 2020), https://verogen.com/gedmatch-incident-response [https://perma.cc/N469-G4KL]. For a period of three hours, "users who did not opt-in for law enforcement matching were available for law enforcement matching, and, conversely, all law enforcement profiles were made visible to GEDmatch users." *Id.* While the company has stated that "[n]o user data was downloaded or compromised," the extent to which law enforcement agencies had expanded access to the resource while permissions were incorrectly set is unclear. *See id.*

128. Hill & Murphy, *supra* note 5.

129. *See supra* note 7; *see also* Andelka M. Phillips, *Data on Direct-to-Consumer Genetic Testing and DNA Testing Companies*, ZENODO (Feb. 19, 2018), https://zenodo.org/record/1183565#.XkBSnC2ZNp8 [https://perma.cc/CCC3-N75K].

130. Andelka M. Phillips, *Only a Click Away — DTC Genetics for Ancestry, Health, Love . . . and More: A View of the Business and Regulatory Landscape*, 8 APPLIED & TRANSLATIONAL GENOMICS 16, 17–20 (2016).

generated as a result of these tests,[131] and the terms and conditions that govern that data, vary widely depending on the nature of the testing and on the company utilized.[132]

A 2017 survey of privacy policies of ninety U.S.-based DTC-GT entities revealed that most of them provide very little information regarding how they deal with law enforcement requests, with many simply stating that data may be disclosed "as required by law" or in response to a warrant, subpoena, or court order.[133] Only a handful of industry leaders—23andMe,[134] Ancestry,[135] and until recently, FamilyTreeDNA[136]—release transparency reports that describe law enforcement requests for information. A few leading companies also provide guides for law enforcement that describe their practices when dealing with such requests.[137]

These sources suggest that, up until now, law enforcement has rarely openly sought access to DTC-GT databases. Further, companies such as 23andMe and Ancestry have publicly stated that they will rigorously oppose all law enforcement requests.[138] Their most recent transparency reports state that, while they have received several requests for genetic and nongenetic data, no genetic data have been

131. *What Are the Types of Genetic Tests?*, NAT'L INSTS. OF HEALTH 5–6 (Aug. 17, 2020), https://ghr.nlm.nih.gov/primer/testing.pdf [https://perma.cc/947S-6Z3P].

132. Hazel & Slobogin, *supra* note 23, at 47–57.

133. *Id.* at 56–57 (describing the law enforcement provisions in the privacy policies and terms and conditions of ninety U.S. DTC-GT companies).

134. *Transparency Report*, 23ANDME, https://www.23andme.com/transparency-report [https://perma.cc/87GC-RCVE] (last updated Nov. 13, 2020).

135. *Ancestry Transparency Report*, ANCESTRY (July 10, 2020), https://www.ancestry.com/cs/transparency [https://perma.cc/CV4E-S7KP].

136. *See Family Finder*, FAMILYTREEDNA, https://www.familytreedna.com/products/family-finder [https://perma.cc/T4NL-HJP7].

137. *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide [https://perma.cc/66DD-KT2V]; *Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/cs/legal/lawenforcement [https://perma.cc/4R78-QMHA]; *FamilyTreeDNA Law Enforcement Guide*, FAMILYTREEDNA, https://www.familytreedna.com/legal/law-enforcement-guide [https://perma.cc/4WSM-3B22].

138. *See* Peter Aldhous, *A Court Tried To Force Ancestry.com To Open Up Its DNA Database to Police. The Company Said No.*, BUZZFEED NEWS (Feb. 3, 2020, 7:11 PM), https://www.buzzfeednews.com/article/peteraldhous/ancestry-dna-database-search-warrant [https://perma.cc/V8PJ-GLKR] ("Ancestry and its main competitor, 23andMe . . . have publicly vowed to defend their customers' genetic privacy, and say they will fight efforts to open up their databases to searches by police.").

released.[139] The one exception comes from Ancestry, which stated that it disclosed consumer genetic information in response to "a 2014 search warrant ordering [the company] to provide the identity of a person based on a DNA sample that had previously been made public for which the police had a match."[140]

However, not all companies are so reluctant to share information. In February 2019, the *New York Times* reported that, unbeknownst to its users, FamilyTreeDNA had been voluntarily providing the Federal Bureau of Investigation ("FBI") with access to its services.[141] Specifically, the company allowed law enforcement to create accounts[142] and utilize a version of its "Family Finder" service, which allows consumers to locate potential genetic relatives in a manner similar to GEDmatch.[143] Further, FamilyTreeDNA did not disclose its cooperation with the FBI in its subsequent transparency report, which it removed only after the revelations by the *Times*.[144]

Like GEDmatch, FamilyTreeDNA was ultimately forced to change its policies in response to consumer backlash. But rather than retreating from its previous stance as GEDmatch did, FamilyTreeDNA has since embraced its role as a tool for law enforcement. In a new media campaign featuring the father of Elizabeth Smart—a woman who was kidnapped at age fourteen and whose abductor and rapist was identified through DNA[145]—the

139. *See, e.g.*, *id.* ("Ancestry received one request seeking access to Ancestry's DNA database through a search warrant . . . Ancestry challenged the warrant on jurisdictional grounds and did not provide any customer data in response."). In 2019, a Pennsylvania court issued a search warrant that would have given law enforcement access to Ancestry's entire database. Ancestry is opposing the warrant in a case that may end up in the Supreme Court. *See id.*

140. *Ancestry 2015 Transparency Report*, ANCESTRY (2015), https://www.ancestry.com/cs/transparency-2015 [https://perma.cc/GFY4-DYKX].

141. Matthew Haag, *FamilyTreeDNA Admits To Sharing Genetic Data with F.B.I.*, N.Y. TIMES (Feb. 4, 2019), https://nyti.ms/2DVnK3x [https://perma.cc/B556-9AYB].

142. *Id.* ("[T]he F.B.I. will have access to its website like any other user . . . .").

143. *See Family Finder*, FAMILYTREEDNA, https://www.familytreedna.com/products/family-finder [https://perma.cc/T4NL-HJP7].

144. Since the publication of the *Times* report, FamilyTreeDNA's "Law Enforcement Guide" has stated that the company "is working on publishing an updated report that will contain details on law enforcement requests submitted through a valid court order, valid trial, grand jury, subpoena, or search warrant for additional personal or genetic information." *FamilyTreeDNA Law Enforcement Guide*, *supra* note 137.

145. Brady McCombs, *Elizabeth Smart Backs Measure To Speed Up DNA Testing*, AP NEWS (July 6, 2017), https://apnews.com/fd693564b0b04cf9a1fb6b52ca722af7 [https://perma.cc/9SQC-ZCKS].

company encourages individuals to upload genetic information that has been profiled by other companies free of charge if they would like to assist in criminal investigations.[146] Thus, unlike GEDmatch, FamilyTreeDNA automatically opts out only existing users residing in the European Union; other existing users must choose to opt out.[147] New users are given the option of allowing their information to be used for law enforcement searches, and the company has reported that most have done so.[148]

The Supreme Court has not yet ruled on the use of forensic genetic genealogy in connection with either public services like GEDmatch or private DTC-GT companies. Although legal scholars raise many of the same Fourth Amendment arguments that are aimed at familial searches of government-run databases,[149] as of now company privacy policies and terms of service or law enforcement's self-imposed limitations serve as the primary barrier to law enforcement access to these resources. Not only do these policies vary significantly among companies, they are generally subject to change at any time,[150] as illustrated by the evolution of the GEDmatch and FamilyTreeDNA protocols dealing with law enforcement. Most importantly, even if these private databases do not give consumers the option of facilitating law enforcement investigations, police agencies might still seek to bypass access restrictions by posing as a civilian consumer, as they did in the GSK case.

In some jurisdictions, however, law enforcement policies might restrict such access. For instance, effective November 1, 2019, DOJ requires federal investigators—as well as state law enforcement agencies

146. *You Can Help*, FAMILYTREEDNA, https://www.familytreedna.com/join [https://perma.cc/4X5S-6DQL]; *Ed Smart, Father of Elizabeth Smart Teams Up with FamilyTreeDNA*, PR NEWSWIRE (Mar. 26, 2019, 3:59 PM), https://prn.to/2Z5QgcZ [https://perma.cc/2QNG-7P5U].

147. Adam Vaughan, *Home DNA-Testing Firm Will Let Users Block FBI Access to Their Data*, NEW SCIENTIST (Mar. 13, 2019), https://www.newscientist.com/article/2196433-home-dna-testing-firm-will-let-users-block-fbi-access-to-their-data [https://perma.cc/KQT5-NK39] (reporting that the company automatically opts-out users from the European Union, while requiring users in the United States to take affirmative action if they wish to opt-out).

148. Amy Dockser Marcus, *Customers Handed Over Their DNA: The Company Let the FBI Take a Look.*, WALL ST. J. (Aug. 22, 2019, 12:26 PM), https://www.wsj.com/articles/customers-handed-over-their-dna-the-company-let-the-fbi-take-a-look-11566491162 [https://perma.cc/M6QA-E4JA] (reporting that only about 2 percent of users opted out in the five months following the policy change).

149. *See supra* note 94 and accompanying text; *see also* Abrahamson, *supra* note 60, at 2553–55.

150. Hazel & Slobogin, *supra* note 23, at 49, 57.

that receive or utilize DOJ funding to engage in forensic genetic genealogy—to identify themselves to any service they use, whether public or private.[151] Accordingly, the type of investigation carried out in the GSK case would be prohibited. Further, the policy permits agents to use only those "services that provide explicit notice to their service users and the public that law enforcement may use their service sites to investigate crimes or to identify unidentified human remains."[152] That language limits DOJ's access to GEDmatch's reduced database as well as to private companies like FamilyTreeDNA that require consumers to consent to law enforcement use of their databases.

4. *Health Care Providers.* Police officers or prosecutors may also seek to compel disclosure of genetic information held by a health care provider or contained within an electronic health record.[153] Given the nature of existing health care databases and the decentralized nature of many electronic medical records, these requests are likely to be targeted, suspect-driven requests for information about a particular individual, as opposed to the large-scale matching queries of resources like GEDmatch and FamilyTreeDNA that are described above. Even here, however, there are few constraints on police access.

Under the Health Insurance Portability and Accountability Act ("HIPAA"), protected health information, including genetic information, may be disclosed to law enforcement pursuant to a "court order or court-ordered warrant," "a subpoena or summons issued by a judicial officer," or a "grand jury subpoena."[154] Genetic information may also be disclosed in response to an "administrative request"[155] if "(1) [t]he information sought is relevant and material to a legitimate law enforcement inquiry; (2) [t]he request is specific and limited in

151. DEP'T OF JUST., UNITED STATES DEPARTMENT OF JUSTICE INTERIM POLICY: FORENSIC GENETIC GENEALOGICAL DNA ANALYSIS AND SEARCHING 2, 6 (2019) [hereinafter DOJ INTERIM POLICY], https://www.justice.gov/olp/page/file/1204386/download [https://perma.cc/CK7R-EZ7A].

152. *Id.* (footnote omitted).

153. *See generally When Does the Privacy Rule Allow Covered Entities To Disclose Protected Health Information to Law Enforcement Officials?*, DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html [https://perma.cc/3X6L-R6E8] (summarizing circumstances in which records can be disclosed to law enforcement).

154. 45 C.F.R. § 164.512(f)(1)(ii)(A)–(B) (2020).

155. "An administrative request[] includ[es] an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law . . . ." *Id.* § 164.512(f)(1)(ii)(C).

scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (3) [d]e-identified information could not reasonably be used."[156] In short, a warrant is not necessarily required to obtain genetic information from a health care provider under HIPAA.[157] Given the diversity of HIPAA-covered entities and the fact that many of them do not publicly disclose law enforcement's requests for data, the extent to which law enforcement takes advantage of the compelled-disclosure provisions of HIPAA is unknown.

If such compelled disclosure were sought, however, it probably does not violate the Fourth Amendment to proceed without a warrant. While that result may seem startling, it is the logical consequence of the Supreme Court's third-party doctrine. Unless a doctor seeks genetic information at the government's behest,[158] the Fourth Amendment is not implicated, because a patient assumes the risk that the doctor, like the person's bank or phone company, will provide the content of medical records to the government.

5. *Researchers.* Research datasets, like those used in precision medicine initiatives, represent still another valuable potential resource of genetic information. For example, the National Institute of Health's *AoU* Research Program, which is featured in the introductory hypothetical, is currently recruiting one million Americans to undergo genetic testing and share their medical records for research.[159] To date, over half of the two hundred thousand-plus individuals who have been recruited come from populations that are historically underrepresented in research datasets,[160] including racial and sexual minority groups.[161]

As with health care databases and electronic medical records, research databases are perhaps most likely to be the subject of targeted, suspect-driven requests for information about a particular research participant. Although certain research databases could

156. *Id.*

157. *But see id.* § 164.512(f)(2)(ii) (setting explicit limitations on the sharing of DNA-related information when disclosures are not compelled by law or legal process).

158. *See* Ferguson v. City of Charleston, 532 U.S. 67, 80–81 (2001) (finding that a policy allowing drug testing of pregnant women violated the Fourth Amendment, but only because the police were involved in devising and implementing the policy).

159. *The Future of Health Begins with You*, NAT'L INSTS. OF HEALTH ALL OF US RSCH. PROGRAM, https://allofus.nih.gov [https://perma.cc/5893-GVB3].

160. Denny, *supra* note 10.

161. All of Us Rsch. Program Investigators, *The "All of Us" Research Program*, 381 NEW ENG. J. MED. 668, 669 (2019).

possibly be used for large-scale familial searches of the type currently being performed using GEDmatch and FamilyTreeDNA, no reports of such activity have surfaced. Indeed, data in research databases are generally de-identified—that is, stripped of personally identifiable information—and would be of limited utility to law enforcement unless it could be relinked to an individual.[162]

In any event, many of these research datasets are more heavily protected from compelled disclosure than the databases of DTC-GT companies or health care providers under HIPAA. The 21st Century Cures Act empowers the Secretary of Health and Human Services to convey CoCs to researchers "engaged in biomedical, behavioral, clinical, or other research in which identifiable, sensitive information is collected (including research on mental health and research on the use and effect of alcohol and other psychoactive drugs)."[163] In theory, if shielded by a CoC, researchers may not be compelled "in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding" to identify individuals who are the subject of such research.[164] Research efforts funded by the National Institutes of Health and other agencies within the U.S. Department of Health and Human Services ("HHS"), such as the *AoU* Research Program, are automatically issued a CoC.[165]

Not all research databases are protected to the same extent, however. Nonfederally funded researchers must apply for a certificate on a case-by-case basis, meaning that many research datasets may remain unprotected.[166] Furthermore, even the enhanced protections conveyed by the Cures Act remain largely untested in the courts.[167] Prior to its implementation, at least one court had enforced a subpoena

---

162. Ellen Wright Clayton & Bradley A. Malin, *Assessing Risks to Privacy in Biospecimen Research*, *in* SPECIMEN SCIENCE: ETHICS AND POLICY IMPLICATIONS 143, 144–149 (2017) (describing the risks and likelihood of re-identification of individuals from biomedical datasets, including by law enforcement).

163. 21st Century Cures Act, Pub. L. No. 114-255, sec. 2012(a), 130 Stat. 1033, 1049 (2016) (codified at 42 U.S.C. § 241(d)(1)(A)).

164. 42 U.S.C. § 241(d)(1)(D) (2018).

165. *Id.* § 241(d)(1)(A)(i); *see Notice of Changes to NIH Policy for Issuing Certificates of Confidentiality*, NAT'L INSTS. OF HEALTH (Sept. 17, 2017), https://grants.nih.gov/grants/guide/notice-files/NOT-OD-17-109.html [https://perma.cc/JT78-T4S2] (explaining implementation of the 21st Century Cures Act).

166. *See Who Can Get a Certificate of Confidentiality?*, NAT'L INSTS. OF HEALTH, https://grants.nih.gov/policy/humansubjects/coc/who-can.htm [https://perma.cc/PC5C-C5TL].

167. Wolf & Beskow, *supra* note 12, at 2681.

overriding the protections of a certificate.[168] Even if law enforcement were limited to de-identified data, there remains a possibility that it could be relinked to the corresponding individuals.[169] And, again, a strict interpretation of the third-party doctrine would deny Fourth Amendment protection against such access.

6. *Surreptitious Collection and Analysis of DNA.* Law enforcement may also engage in surreptitious collection of DNA in the course of a criminal investigation, as occurred in our introductory hypothetical. This practice can occur independently of, or in conjunction with, other genetic investigatory techniques, such as long-range familial searches of public and private databases. For example, after identifying potential suspects in the GSK case using GEDmatch, law enforcement surreptitiously collected the DNA of the primary suspect, DeAngelo, first from the door handle of his car, and later from a discarded tissue, and then matched it with crime scene DNA.[170]

While the Supreme Court has not yet addressed the issue of surreptitious collection of DNA by law enforcement, the Court has been reluctant to apply Fourth Amendment protections to "abandoned" property, holding instead that individuals lack a reasonable expectation of privacy in discarded items.[171] As a result, in the majority of jurisdictions, police are generally not required to obtain a warrant or court order before engaging in surreptitious collection of

168. State v. Bradley, 634 S.E.2d 258, 261 (N.C. Ct. App. 2006) (vacating a trial court's order to disclose research records to defense counsel for lack of materiality, but also noting that "[t]he trial court's order effectively requires [a research entity] to disclose information concerning the research subject's privacy which it is obliged, pursuant to the Certificate of Confidentiality and federal statutes, to protect"); *see* Leslie E. Wolf, Mayank J. Patel, Brett A. Williams Tarver, Jeffrey L. Austin, Lauren A. Dame & Laura M. Beskow, *Certificates of Confidentiality: Protecting Human Subject Research Data in Law and Practice*, 43 J.L. MED. & ETHICS 594, 597 (2015).

169. Khaled El Emam, Sam Rodgers & Bradley Malin, *Anonymising and Sharing Individual Patient Data*, BMJ, Mar. 20, 2015, at 2–5, https://www.bmj.com/content/bmj/350/bmj.h1139.full.pdf [https://perma.cc/5J72-RNUV].

170. Nancy Dillon, *Golden State Killer Suspect Arrested After Cops Swiped His DNA from Car Door Handle and Tissue*, N.Y. DAILY NEWS (June 1, 2018, 6:55 PM), http://www.nydailynews.com/news/crime/ny-news-golden-state-killer-dna-collected-car-door-trash-20180601-story.html [https://perma.cc/ER9L-VBSL].

171. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 40–41 (1988) (holding that inspection of discarded garbage by police does not constitute a search because "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public" (footnotes omitted)).

DNA.[172] In addition, state laws that place restrictions on surreptitious collection and analysis of genetic material without consent generally contain exceptions for law enforcement.[173] And while the aforementioned DOJ Interim Policy prohibits covert collection of DNA samples from relatives of a suspect—as opposed to the suspect themselves—the guidelines allow prosecutors to override that restriction if they have "reasonable grounds to believe that [seeking informed consent] would compromise the integrity of the investigation."[174] This language gives prosecutors wide leeway to authorize covert collection of DNA.

7. *Summary.* The foregoing discussion makes clear that there are two principal situations in which the police might seek DNA for investigative purposes. The first might be called "suspect-based." In this situation, the police have a suspect and want to obtain his or her DNA, most likely either from the suspect or from the suspect's health care provider or from a discarded item. In the second situation, which might be called "profile-based," the police have a DNA profile from a crime scene and want to access a government, public, or private database to determine whether there is a match or a partial match. Other than when the police seek DNA directly from a person who has not been arrested—a scenario that would probably require a warrant, given *King*'s distinction between those who have been arrested and those who have not[175]—current Fourth Amendment jurisprudence has

172. Joh, *supra* note 49, at 699 & n.197 ("In cases of surreptitious sampling, the few decided cases have analogized genetic information left behind on everyday objects to garbage, and thus open for police collection without a warrant, individualized suspicion, or consent."); Albert E. Scherr, *Genetic Privacy & the Fourth Amendment: Unregulated Surreptitious DNA Harvesting*, 47 GA. L. REV. 445, 452 (2013) ("[T]he police are beginning to use the technique more frequently."); Nicolle K. Strand, *Shedding Privacy Along with Our Genetic Material: What Constitutes Adequate Legal Protection Against Surreptitious Genetic Testing?*, 18 AM. MED. ASS'N J. ETHICS 264, 268–69 (2016) (noting Alaska's state law exemption for surreptitious genetic testing by law enforcement).

173. *See, e.g.*, ALASKA STAT. § 18.13.010(b)(2) (2018) (exempting "DNA samples collected and analyses conducted . . . for a law enforcement purpose, including the identification of perpetrators and the investigation of crimes and the identification of missing or unidentified persons or deceased individuals"); *see also* GENETICS & PUB. POL'Y CTR., STATE LAWS PERTAINING TO SURREPTITIOUS DNA TESTING *passim* (2009), https://web.archive.org/web/20150306044016/http:/www.dnapolicy.org/resources/State_law_summaries_final_all_states.pdf [https://perma.cc/6ULK-CPDR] (identifying which state laws exempt law enforcement activities).

174. *See* DOJ INTERIM POLICY, *supra* note 151, at 6.

175. Maryland v. King, 569 U.S. 435, 463 (2013) (emphasizing the diminished expectation of privacy of arrestees). Most lower courts have so held. *See, e.g.*, Bill v. Brewer, 799 F.3d 1295, 1301–

little to say about any of these different types of law enforcement collection of and access to genetic information. Our empirical study was designed to cast further light on whether that should change.

II. METHODOLOGY

Our goal in this study was to begin an inquiry into societal views about the types of genetically focused law enforcement investigations that were described in Part I. The Supreme Court has made clear that Fourth Amendment analysis is governed by privacy expectations, specifically by expectations of privacy society is prepared to recognize as reasonable.[176] Thus, the aggregate views of the citizenry are, at the least, relevant to the Fourth Amendment question of when a search has occurred, a point we revisit in the Conclusion.

This study builds on a survey methodology initially pioneered by Professor Christopher Slobogin, a co-author of this Article, and Joseph E. Schumacher,[177] later modified and extended by Slobogin[178] and others,[179] to gauge the intrusiveness of various law enforcement searches and government activities such as surveillance and data mining. The basic idea is simple: present a representative sample of the population with scenarios from court decisions, or variations thereof, and ask the subjects to rate their "intrusiveness." The latter word was intentionally chosen as the dependent variable because it captures both the property and the privacy components of Fourth Amendment analysis,[180] and because, along with its cousin "invasiveness," it is

02 (9th Cir. 2015) (assuming a warrant is required in this situation even when subject is not suspected of a crime); Friedman v. Boucher, 580 F.3d 847, 856–58 (9th Cir. 2009) (holding that, in the absence of a statute, status as a pretrial detainee did not justify warrantless, compelled collection of DNA); State v. Lee, 976 So. 2d 109, 123–24 (La. 2008) ("When the facts of the present case are compared to the aforementioned jurisprudence of other courts, we find the collection of defendant's DNA constituted a search.").

176. *See supra* text accompanying note 34.

177. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society*," 42 DUKE L.J. 727, 733–37 (1993).

178. Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 275–80 (2002); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 333–36 (2008).

179. *See, e.g.*, Bernard Chao, Catherine Durso, Ian Farrell & Christopher Robertson, *Why Courts Fail To Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 294–97 (2018).

180. *Cf.* United States v. Jones, 565 U.S. 400, 409 (2012) ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to,* not *substituted for,* the common-law trespassory test.").

frequently used by the Supreme Court itself in describing the scope of the Fourth Amendment.[181]

In this study, however, we also asked a follow-up question explicitly using "expectations of privacy" language. Research relying on this type of methodology has tended to show that the Supreme Court's assumptions or assertions about privacy expectations are frequently inconsistent with societal views.[182] We wanted to inquire whether this was true of scenarios involving government collection of and access to genetic information, specifically DNA profiles for identification purposes.

A. Survey Creation and Validation

The materials for this research were developed in coordination with an interdisciplinary working group consisting of scholars from the law, medicine, psychology, history, economics, and humanities fields.[183] In order to validate the surveys, we conducted two pilot tests: first with a group of approximately seventy graduate students at Vanderbilt Law School and then with approximately two hundred individuals on Amazon Mechanical Turk ("MTurk"). Respondents were given the opportunity to provide feedback on the surveys and describe any areas of confusion or technical difficulties that they encountered. Feedback revealed several areas of ambiguity and the scenarios were modified accordingly before being administered to the full set of participants.

The final surveys consisted of twenty-one short scenarios describing law enforcement access either to genetic data or to other types of personal information, such as the contents of a bedroom, text messages, or web-browsing history. Appendix A contains the complete scenarios. Nine of the scenarios involved police collection of or access to DNA. The other twelve described other types of police searches. While our primary goal was to evaluate privacy expectations in connection with the DNA-related scenarios, we included the other scenarios for comparison purposes. Particularly important for Fourth

181. *See* Christopher Slobogin, *Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire*, 94 MINN. L. REV. 1588, 1595 (2010) (reporting that these terms have been used in over two hundred Supreme Court Fourth Amendment cases).

182. *See generally* sources cited *supra* notes 177–79179.

183. The survey was circulated to investigators at The Center for Genetic Privacy and Identity in Community Settings (GetPreCiSe) at Vanderbilt University. A complete list of members is available at: https://www.vumc.org/getprecise/person/team [https://perma.cc/W5BN-8UU9].

Amendment analysis were the scenarios involving searching a bedroom, searching emails, performing a pat down (or frisk) and setting up a roadblock. The Supreme Court has held that all four of these scenarios are governed by the Fourth Amendment. The first two require probable cause (and a warrant in non-exigent circumstances),[184] the pat down requires reasonable suspicion,[185] and the roadblock requires individualized suspicion or a neutral plan,[186] depending on whether it is aimed at "ordinary crime control"[187] or is more regulatory in orientation.[188]

The use of single-sentence scenarios allowed us to gather responses on a broad range of law enforcement activities in a short period of time. While this type of query obviously does not provide full context to the subjects, it does provide a description that is consistent with "black letter law" on the Fourth Amendment. For instance, "police looking at all of the text messages that a person has sent or received" on his or her phone in the absence of consent describes a situation that, regardless of context, requires probable cause.[189] Similarly, "police getting a person's DNA profile from a genetic testing company (such as Ancestry or 23andMe) that the person has used in the past" describes a situation currently governed by the third-party doctrine.[190] We hoped a comparison of the intrusiveness ratings of these types of scenarios would help us determine how society views genetic investigations relative to other investigations known to be governed by the Fourth Amendment.

---

184. Chimel v. California, 395 U.S. 752, 763–64 (1969) (holding that the search of a home requires a warrant in non-exigent circumstances); Berger v. New York, 388 U.S. 41, 44, 63–64 (1967) (holding that interception of electronic communications requires a warrant).

185. Terry v. Ohio, 392 U.S. 1, 30 (1968).

186. *Compare* City of Indianapolis v. Edmond, 531 U.S. 32, 44, 47 (2000) ("When law enforcement authorities pursue primarily general crime control purposes at checkpoints . . . , stops can only be justified by some quantum of individualized suspicion."), *with* United States v. Martinez-Fuerte, 428 U.S. 543, 566 (1976) ("[S]tops for brief questioning routinely conducted at permanent checkpoints are consistent with the Fourth Amendment and need not be authorized by warrant.").

187. *Edmond*, 531 U.S. at 44, 47 ("Of course, there are circumstances that may justify a law enforcement checkpoint where the primary purpose would otherwise, but for some emergency, relate to ordinary crime control.").

188. *See Martinez-Fuerte*, 428 U.S. at 545, 566 ("We also hold that the operation of a fixed checkpoint need not be authorized in advance by a judicial warrant."). *But see id.* at 567 ("[O]ur holding today is limited to the type of stops described in this opinion."); *Edmond*, 531 U.S. at 43 ("[T]he border context . . . was crucial in *Martinez-Fuerte*.").

189. Riley v. California, 573 U.S. 373, 403 (2014).

190. *See supra* Part I.A.2.

To gain a more nuanced understanding of the factors influencing participants' attitudes, we employed five closely related versions of the survey. Some empirical work has suggested that people's views about the intrusiveness of police actions might vary, depending both on whether their privacy, as opposed to someone else's, is invaded by the police action, and on the reason for that action.[191] Thus, in addition to a baseline survey, which simply told the participants the police were looking for evidence of an unspecified crime committed by an unspecified person, we constructed four other surveys with slightly different instructions that varied: (i) the subjects' perspective by asking them to assume that they, rather than an unidentified person, were the target of the police action (first-person condition); (ii) the goal of the police action, with one variation asking participants to assume (a) that police were looking for evidence of serious crime (serious-crime condition) and the other (b) that police were trying to *prevent* a serious crime (crime-prevention condition); and (iii) whether evidence was *found* during the police action rather than merely searched for (hindsight-bias condition). A detailed summary of the experimental variations is found in Appendix B.

Once the scenarios were constructed, electronic survey instruments were created using the Research Electronic Data Capture ("REDCap") tools hosted at Vanderbilt University. In Part I of the survey, participants were asked to rank each scenario on a 100-point scale ranging from "not intrusive at all" (0) to "extremely intrusive" (100). In Part II, participants were presented with the same twenty-one scenarios and asked whether each scenario described a situation in which a person was entitled to a "reasonable expectation of privacy" (yes/no). In both parts, participants were instructed to read all twenty-one scenarios carefully before answering and were told they could go back and change their answers after reading and responding to other scenarios. However, once in Part II, participants could not go back to Part I.

B. Study Population and Demographics

Participants were recruited via MTurk, an online crowdsourcing marketplace,[192] and paid one dollar following successful completion of

191. *See* Slobogin & Schumacher, *supra* note 177, at 765–68 (advancing "inference of guilt" and "dangerousness" theories as to why certain scenarios were rated as relatively less intrusive in the third-person scenarios).

192. *Overview*, AMAZON MECHANICAL TURK, https://www.mturk.com [https://perma.cc/2MH9-ABQY].

one of the five variations of survey. The surveys were administered over the course of two weeks in December 2018 and were limited to subjects who had not previously taken any of the other variations of the survey. The average time respondents spent completing the surveys was 13.8 minutes.

The 1,597 respondents represented a diverse population that included significant ranges in age, education level, socioeconomic status, political affiliation, and religiosity. In summary, 1,257 respondents identified as white (78.7%), 180 as Black or African American (11.3%), 79 as Asian (4.9%), and 22 as American Indian or Alaska Native (1.4%). Responding to a separate question, 172 respondents reported Hispanic, Latino, or Spanish origin (10.7%). The majority characterized their previous interactions with law enforcement as either "all positive" (362; 22.7%) or "mostly positive" (629; 39.4%), and their neighborhood as "low crime" (1,148; 71.9%). A small number of participants reported having previously undergone genetic testing through a doctor (143; 9.0%), DTC-GT company (185; 11.6%), or as part of a research study (92; 5.8%), although the vast majority reported no previous testing (1,177; 73.7%). A complete list of the demographic information is found in Appendix C.

C. Limitations

We note that MTurk workers, while demographically diverse in many respects, tend to be predominately white, and are generally younger, more highly educated, and more computer literate when compared to the entire U.S. population.[193] Indeed, Professors Matthew B. Kugler and Lior Jacob Strahilevitz have observed that "Mechanical Turk respondents are significantly more privacy-protective than the general U.S. population, perhaps because they skew younger."[194] As a result, they conclude that "one should not use Mechanical Turk samples to assess the base-rate support for privacy-related beliefs in the general population."[195] But they also state that MTurk "may . . . still

193. Joel Ross, Andrew Zaldivar, Lilly Irani & Bill Tomlinson, *Who Are the Crowdworkers? Worker Demographics in Amazon Mechanical Turk*, *in* CHI 2010: PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 2863, 2865–68 (2010), http://web.mit.edu/2.744/www/resourceMaterials/otherResources/p2863-ross.pdf [https://perma.cc/852C-X5JM].

194. Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205, 233 n.113.

195. *Id.*

be valid to use such samples to evaluate the *relative* intrusiveness of searches"[196] as we do here.

Recently, some concern has been expressed about international MTurk workers gaining access to surveys designed for U.S. participants through the use of "virtual private networks" ("VPNs").[197] There are indications that these participants produce lower quality responses, perhaps because they are more likely to employ "bots" or "scripts" to rapidly complete surveys.[198] Since we relied on the Amazon platform to screen in only U.S. participants and did not personally collect or verify their IP addresses, we are unable to rule out the possibility that a subset of participants accessed our surveys in such a manner, nor were we able to assess retroactively the extent to which it occurred. The countermeasures suggested by some scholars, such as requiring all participants to turn off VPNs and excluding those who do not,[199] may also introduce bias, as such measures are likely to exclude privacy-conscious U.S. participants who utilize VPNs for legitimate, privacy-protective reasons. In an effort to mitigate the concerns described above, we excluded all responses received in under five minutes (5.1% of responses; 86 of 1,683 participants), as these response times are indicative that the individual did not answer thoughtfully, but rather simply "clicked through" the survey or used a "bot" or "script" to rapidly generate responses.[200]

D. Hypotheses

In constructing this study, we started with four general hypotheses. First, based on the findings of other research in a similar vein,[201] we expected that our survey participants' intrusiveness ratings and conclusions about expectations of privacy would bear little relation to whether the information or items described in a scenario had been surrendered or was in the possession of a third party, in contrast to the

196. *Id.*

197. Ryan Kennedy, Scott Clifford, Tyler Burleigh, Philip D. Waggoner, Ryan Jewell & Nicholas J. G. Winter, *The Shape of and Solutions to the MTurk Quality Crisis*, 8 POL. SCI. RES. & METHODS 2–4 (2020), https://www.cambridge.org/core/services/aop-cambridge-core/content/view/521AEEB9A9753D5C6038440BD123826C/S2049847020000060a.pdf [https://perma.cc/7M6T-YLYJ].

198. *Id.* at 3–14.

199. *Id.* at 14–16.

200. After excluding responses received in under five minutes, the average time respondents spent completing the surveys was 19.4 minutes.

201. *See* sources cited *supra* notes 177–79.

Supreme Court's third-party doctrine, which often makes this fact dispositive in finding that no search is involved. Second, given the intimate, personal nature of DNA, we hypothesized that most of our genetically focused investigations would be viewed as among the most intrusive of our twenty-one scenarios. Third, we expected that participants in the "third-person" condition would assign lower intrusiveness ratings to the scenarios than those in the "first-person" condition. Fourth, on the theory that police actions would be viewed as less intrusive if they occur for a particularly "good reason," we hypothesized that participants who were asked to assume the police were looking for evidence of *serious* crime, asked to assume the goal of the action was *prevention* of serious crime, or asked to assume that the police actually *found* the evidence they were looking for, would assign lower intrusiveness ratings than those who were given scenarios that simply indicated the police were looking for evidence of an unspecified crime.

III. RESULTS

This Part first describes the results from our baseline survey, and then describes the results from the other four surveys. As outlined in Section A, the results provide significant support for our first two hypotheses but, as described in Section B, only marginal support for our third hypothesis and much less support of our fourth hypothesis.

A. Baseline Survey

In the baseline survey, scenarios were presented in the third person, meaning that the police action was directed at someone other than the subject. Participants were also told that police were engaging in the action to locate "evidence of some type of criminal activity." Finally, as was the case with all variations of the survey, participants were told that the subject of the search was presumed innocent and did not consent to the search.

Table 1 shows the mean intrusiveness rating of each scenario, along with a confidence interval ("Z") indicating the extent to which a given mean intrusiveness rating can be said to differ from adjacent ratings. The final column indicates the percentage of subjects who

TABLE 1: INTRUSIVENESS AND EXPECTATIONS OF PRIVACY IN 21 SCENARIOS

Baseline Survey: 3rd Person *n = 323*		**Intrusiveness**			**REP?**
#	**Scenario:**	**Mean**	**Z**	**S.D.**	**% Yes**
1	Genetic Data from Doctor	76.0	± 2.6	24.2	84.2%
2	Medical Records	74.8	± 2.6	23.7	82.7%
3	Bedroom Search	74.0	± 2.6	23.8	74.9%
4	Text Messages	72.7	± 2.4	22.4	77.7%
5	Familial Search of Public Genealogy DNA DB	72.1	± 3.2	29.6	69.0%
6	Genetic Data from DTC-GT Company	71.9	± 2.7	24.9	74.9%
7	Emails	71.9	± 2.4	21.8	76.2%
8	Financial Records	70.8	± 2.5	23.3	74.6%
9	Collection for a Universal DNA DB	69.3	± 3.4	30.8	64.1%
10	Genetic Data from Researchers	69.0	± 3.0	27.1	76.8%
11	Web History	66.7	± 2.7	24.4	70.3%
12	Phone Numbers	63.2	± 2.7	24.6	70.3%
13	Social Media	62.1	± 2.8	25.7	63.2%
14	Universal Fingerprint DB	60.6	± 3.5	32.5	61.3%
15	Cell Location	60.3	± 2.8	25.6	65.9%
16	Pat Down	55.7	± 2.9	27.0	44.9%
17	Surreptitious Collection of Discarded DNA	50.2	± 3.3	30.3	42.4%
18	Compelled DNA Collection from Arrestees	49.1	± 3.4	31.5	41.2%
19	Roadblock	39.4	± 3.0	27.4	24.1%
20	Familial Search of Forensic DNA DB	38.9	± 3.4	31.3	33.7%
21	Search for Suspect in Forensic DNA DB	32.8	± 3.2	29.6	29.7%

believed that the indicated police action infringed a "reasonable expectation of privacy." The scenarios are ranked from most intrusive to least intrusive based on their mean intrusiveness rating.[202]

Note first that, while the scenarios involving genetic information are spread throughout this hierarchy, many are ranked at the high end. Respondents ranked law enforcement access to genetic information from an individual's doctor as the most intrusive of all the scenarios, just above police access to other information in medical records. Police access to public genealogy, direct-to-consumer and research databases, as well as the creation of a universal DNA database, were also ranked among the most intrusive activities, on a par with searches of bedrooms, text messages, and emails, although the public and universal databases received a lower percentage of positive responses on the expectation of privacy query than these other scenarios.

These findings support our first hypothesis. The fact that genetic information resides with a third party does not appear to be an important consideration when people are asked about the privacy of that information or police access to it. The findings also clearly support our second hypothesis. Many types of genetically focused investigations are perceived to be as intrusive as searches that are clearly governed by the Fourth Amendment and that require a warrant based on probable cause.

At the same time, our findings do not support a claim for "genetic exceptionalism," the notion that DNA is so private that obtaining it should always require a warrant. In fact, many scenarios involving forensic uses of genetic material were ranked among the least intrusive, including those describing surreptitious collection of DNA, compelled collection of DNA from arrestees, and law enforcement searches of government-run forensic databases to locate suspects or relatives of suspects. All of these scenarios were viewed as less intrusive than a pat

202. We did not find significant demographic differences in terms of mean rankings. However, only a small portion of our sample identified as African American, a population that has often expressed more distrust of the police generally and with respect to use of genetic information. *See* Darren Lenard Hutchinson, Who *Locked Us Up? Examining the Social Meaning of Black Punitiveness*, 127 YALE L.J. 2388, 2431 (2018) (reviewing JAMES FORMAN, JR., LOCKING UP OUR OWN: CRIME AND PUNISHMENT IN BLACK AMERICA (2017)) (noting that research shows that "[r]elative to whites, blacks distrust police and believe that officers discriminate on the basis of race"). Demographic differences in attitudes about law enforcement use of genetic information is a fertile avenue for further research.

down, and the latter two were viewed as on par with a roadblock in terms of intrusiveness. Further, for all of these latter scenarios, well under 50 percent of our participants answered "yes" when asked whether the action infringed a reasonable expectation of privacy. Since DNA is a constant in all of these situations, something else besides the nature of the information being sought is motivating these conclusions—a topic taken up in Part IV.

B. Experimental Manipulations

As detailed above, we developed several variations of the baseline survey: a first-person variation ("police looking for your data" rather than "police looking for a person's data"), a serious-crime variation, a crime-prevention variation, and a hindsight-bias variation. We expected the first variation to produce higher intrusiveness ratings and the other three to produce lower intrusiveness ratings, compared to the baseline scenario. However, with the exception of our first prediction, our hypotheses were not borne out.

With respect to the first-person condition, we observed statistically significant ($p \leq 0.05$) increases in the mean intrusiveness of fourteen out of twenty-one scenarios, a significant decrease in one scenario,[203] and no change in six scenarios.[204] For a subset of scenarios, respondents were also more likely to believe that a reasonable expectation existed when given the first-person perspective; compared to the baseline/third-person condition, we observed statistically significant increases in nine out of twenty-one scenarios, while twelve remained unchanged.[205] As others have noted, this finding that the first-person perspective increases intrusiveness ratings could help explain the current narrow interpretation of the Fourth Amendment's threshold, to the extent judges gauge expectations of privacy from a third-person rather than a first-person perspective.[206]

The findings from the other surveys were less conclusive. We did not observe a statistically significant change in the perceived

203. We observed a statistically significant decrease in the mean intrusiveness rating for the police roadblock scenario.

204. The six scenarios without statistically significant differences ($p > 0.05$) were familial searches of public database, obtaining DNA from a DTC-GT company, creation of a universal forensic database, creation of a universal fingerprint DB, pat down, and compelled collection of DNA from arrestees. *See infra* Table 2.

205. *See infra* Table 2.

206. *See, e.g.*, Slobogin & Schumacher, *supra* note 177, at 760.

intrusiveness of any of the scenarios when participants were instructed that police were "looking for evidence that could help solve a serious crime (such as murder, sexual assault, or terrorism)" as opposed to simply "looking for evidence of some type of criminal activity."[207] Nor did we find noticeable changes in perceived intrusiveness or privacy expectations in the prevention condition or the hindsight-bias condition.[208] The most likely explanation for these null findings is that the participants in each survey used the full 0–100 scale in rating intrusiveness, regardless of their assigned condition. Thus, participants asked to assess the intrusiveness of police efforts to find evidence in a doctor's office ranked that scenario at the high end of the scale whether police were looking for evidence of serious crime, were trying to prevent one, or actually found it. Our between-subjects design did not ask participants to compare intrusiveness under these various conditions, but rather held the relevant condition constant for each of the twenty-one scenarios. This aspect of the methodology turned out to be a poor test of our hypotheses about the impact of the serious-crime, crime-prevention, and hindsight-bias variations.

At the same time, the lack of variation in mean intrusiveness ratings also indicates that the hierarchy of scenarios remained relatively constant between all four third-person surveys (we exclude the first-person survey results here because, as reported above, that methodology resulted in significantly higher intrusiveness ratings). Only five scenarios changed more than two positions up or down in the hierarchy over any of the four third-person survey variations, and no scenario changed more than six positions.[209] Further, these changes were largely the result of very small changes in mean intrusiveness ratings. For instance, the scenario involving the universal DNA database was one of two that changed six positions, but its mean intrusiveness rating only ranged between 68.6 and 73.5 among the four survey variations. Similarly, the text message scenario—the only other scenario that changed six positions—only ranged between 67.1 and 72.7.

207. *See infra* Appendix B (survey variations); Table 3 (results for "serious crime" variation).

208. *See infra* Tables 4–5. For the survey variations, see *infra* Appendix B.

209. *See infra* Tables 2–5.

C. Summary of Results

Our most significant findings as they relate to law enforcement efforts to use DNA for investigative purposes can be reduced to three. First, our subjects saw significant differences in intrusiveness between different types of DNA scenarios. Regardless of variation—third-person surveys versus first-person surveys versus type of police goal—obtaining genetic information from an individual's doctor was ranked as the most intrusive or second most intrusive scenario. In all of the conditions, creating or accessing arrestee databases, including where familial matching was involved, was ranked among the bottom three scenarios. And scenarios accessing public, DTC-GT, and research databases were ranked in the middle of the pack, along with the creation of a universal DNA database. Second, many types of law enforcement DNA inquiries were equated with police actions that clearly implicate the Fourth Amendment. Regardless of experimental condition, accessing DNA in medical records and accessing public, DTC-GT, and research databases were considered to be as intrusive as or more intrusive than searches of bedrooms, texts, emails, and cell-site location data, all of which are searches under the Fourth Amendment requiring probable cause.[210] Third, however, some types of DNA investigations were rated similarly to police investigative techniques that do not require probable cause. Surreptitious collection of DNA and creation of and access to arrestee databases were all seen as less intrusive than a pat down, which only requires reasonable suspicion,[211] and accessing forensic databases was seen as less intrusive than seizures at a roadblock, which the Court has held requires reasonable suspicion if aimed at "ordinary crime control."[212] If replicated, these findings have significant implications for Fourth Amendment jurisprudence.

IV. IMPLICATIONS OF THE RESEARCH

Our findings suggest that, to the extent current Fourth Amendment jurisprudence fails to regulate, or only minimally regulates, genetically focused police investigations, it ignores societal views about privacy, improperly so in our view. In particular, current

210. *See supra* note 184 and accompanying text.

211. Terry v. Ohio, 392 U.S. 1, 30–31 (1968).

212. *See* City of Indianapolis v. Edmond, 531 U.S. 32, 44, 48 (2000).

jurisprudence fails to recognize how important the situs of genetic information is in influencing our participants' privacy expectations. Earlier, we noted the distinction between suspect-driven investigations and profile-driven investigations.[213] We explore the implications of our findings under those two categories.

A. Suspect-Driven Investigations

Assume the police have a named suspect and want to obtain his or her DNA to see if it matches crime scene DNA. There are at least three ways they can accomplish this: requesting or compelling a sample from the suspect; obtaining a sample or profile from another source; or surreptitiously collecting a DNA sample.

1. *Compulsion.* We did not include in our study a scenario that directly tested this situation. As we noted earlier, this type of action would almost certainly require the police to obtain a warrant if the person has not yet been arrested.[214] We did include a scenario involving taking a DNA sample from an arrested individual, as in *King*. However, this scenario was framed as part of a routine "booking" procedure aimed at all arrestees in an effort to populate a forensic database, not as an investigation of a particular suspect. Thus, that scenario is discussed below in connection with collection of DNA for the purpose of creating a database profile.

2. *Third-Party Access.* A second way the police can attempt to obtain the DNA of a named suspect is to go to a third-party source—the person's doctor, a public database, or a private database such as those maintained by health care providers, researchers, or DTC-GT companies. Under the Supreme Court's current third-party doctrine, none of these situations involves a search for Fourth Amendment purposes.[215] Consistent with all of the related research in this area,[216]

213. *See supra* Part I.B.7.

214. *See supra* note 175 and accompanying text.

215. *See supra* Part I.A.2.

216. *See, e.g.*, Christine S. Scott-Hayward, Henry F. Fradella & Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 49–58 (2015) ("Participants in this study felt entitled to high levels of privacy in their digital information, including information . . . covered by the third party doctrine."); *cf.* Jeremy A. Blumenthal, Meera Adya & Jacqueline Mogle, *The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy,"* 11 U. PA. J. CONST. L. 331, 341, 344–54 (2009) ("[E]mpirical research on consent and

however, our survey participants do not agree with the third-party doctrine's application in these types of cases. Police access to a suspect's medical records—as well as to a suspect's financial records—are considered to be more intrusive than a search of a bedroom, which requires a warrant and probable cause. In evaluating intrusiveness, our survey participants appeared to focus not on the risks assumed (real or imagined) when information is given to third parties, but rather on the nature or situs of the information involved—or perhaps both. If our other results, analyzed below, are any indication, the situs of the information—that is, where the information is—appears to be the key consideration.

3. *Surreptitious Collection and Analysis.* A third way the police can obtain the DNA of a named suspect is through obtaining an item discarded by the suspect. Here, the most applicable Supreme Court doctrine has to do with abandoned property, as in cases involving police examination of garbage left at curbside or seizure of items left out in "open fields" that are privately owned but outside the home's curtilage, all of which hold that the Fourth Amendment does not apply.[217] The Court has also made clear that even information that is *not* abandoned is unprotected by the Fourth Amendment if it is "knowingly exposed" to the public.[218]

One could make the argument that, unlike the items seized or the activities viewed in those cases, discarded DNA is not "voluntarily" abandoned or "knowingly" exposed.[219] One could also make the argument, based on the results in *Carpenter* (which involved the seizure

---

perceptions or expectations of privacy . . . suggest[s] that lay perceptions in fact differ from Supreme Court doctrine—at times substantially.").

217. *See supra* Part I.A.1. Some state courts have reached different conclusions. *See, e.g.*, State v. Tanaka, 701 P.2d 1274, 1276–77 (Haw. 1985) ("People reasonably believe that police will not indiscriminately rummage through their trash bags to discover their personal effects."); State v. Goss, 834 A.2d 316, 319 (N.H. 2003) (holding there was a reasonable expectation of privacy in black plastic trash bags on driveways when set "out for regular collection"); State v. Morris, 680 A.2d 90, 96 (Vt. 1996) ("[P]eople reasonably expect that, once their refuse is placed on the curb in the customary and accepted manner, it will be collected, taken to the landfill, and commingled with other garbage without being intercepted and examined by the police."); State v. Hempele, 576 A.2d 793, 810 (N.J. 1990) ("Questions of 'abandonment' and property law do not defeat an expectation of privacy in garbage left on the curb for collection . . . . A person has as much right to privacy in items concealed in a garbage bag as in items concealed in other opaque containers.").

218. *See supra* Part I.A.1.

219. Scherr, *supra* note 172, at 465–68; Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 867 (2006).

of 129 days of location data)[220] and *Jones* (where the Court held that GPS tracking of a car for 28 days is a search),[221] that even information that is knowingly exposed to the public is protected by the Fourth Amendment if its quantity or quality make it particularly revealing. But our survey participants did not seem to be attentive to these issues; rather, they ranked the scenario in which DNA is taken from a discarded item as among the least intrusive, presumably based on the idea that the DNA has been discarded and is found in a public space. The location of the genetic information, not its nature, appears to be the most important consideration.

B. Profile-Driven Investigations

Now assume the police do not have a suspect but rather a DNA profile taken from a crime scene. Here, law enforcement would like to match the profile to profiles in a database. The implications of our results for this purpose are best considered in connection with the four types of DNA databases we studied: government-run databases; public databases (such as GEDmatch); private databases (primarily DTC-GT companies) and research-based databases (such as *AoU*). For each type of database, one can ask: Under what circumstances may a DNA sample be obtained and analyzed to create a profile (the collection question), and when can the DNA that has been collected and profiled be accessed by law enforcement (the access question)? The answers to these questions turn out to be quite different depending on the type of database; more specifically, again, the answers depend on where the DNA is located.

1. *Government-Run Databases.* From a doctrinal point of view, the collection question for government-run databases is partially answered by *King*. Given the emphasis in that case on the lessened privacy interests of jailed individuals,[222] the Court is very likely to hold that taking DNA samples from the general, unincarcerated population is impermissible absent a very significant justification.[223] At the same

220. Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

221. United States v. Jones, 565 U.S. 400, 403–04 (2012).

222. *See supra* note 31 and accompanying text.

223. A stance that calls into question the holding in *King* itself, since the justification for obtaining the DNA of arrestees who are not yet convicted is weak unless first-time arrestees are more likely to commit crime than the general population. *Cf.* J.W. Hazel, E.W. Clayton, B.A.

time, *King* clearly held that the Fourth Amendment is *not* violated by a statute that authorizes jail personnel, acting in the absence of probable cause, to collect DNA samples from people arrested for felonies (and presumably from people convicted of felonies as well) and then profile them.[224] The Court left open the possibility that a statute permitting collection of DNA from persons arrested for minor crimes would not be constitutional,[225] but it is unlikely to so hold.[226]

As to when the government can access the DNA it has collected, *King* indicated law enforcement agencies may do so any time they want to identify an arrestee, as well as any time they have crime scene DNA they think might match a profile in the database.[227] But the Court also made clear that the government cannot access the DNA to discover medical information and the like. The Court emphasized that "the CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee," that "even if non-coding alleles could provide some information, they are not in fact tested for that end," and that the statute ensures that "[n]o purpose other than identification is permissible."[228]

Our survey data are broadly consistent with this actual and predicted case law. Our participants viewed both government creation of an arrestee-based database and government access to that database—whether directly or through familial matching—as similar in intrusiveness to a roadblock and much less intrusive than a pat down, neither of which require a warrant or probable cause.[229] In contrast,

---

Malin & C. Slobogin, *Is It Time for a Universal Genetic Forensic Database?*, 362 SCI. 898, 899 (2018) (describing the discriminatory impact of current testing practices).

224. *See supra* notes 20–23 and accompanying text.

225. *See* Maryland v. King, 569 U.S. 435, 465 (2013) (describing the holding in the context of "an arrest supported by probable cause to hold for a *serious* offense" (emphasis added)); *id.* at 480 (Scalia, J., dissenting) ("[T]he Court's holding will result in the dumping of a large number of arrestee samples—many from minor offenders—onto an already overburdened system . . . .").

226. *See* Florence v. Bd. of Chosen Freeholders, 566 U.S. 318, 322, 339 (2012) (allowing body cavity searches of individuals arrested for minor crimes, even in the absence of any suspicion of contraband, because the record lacked "substantial evidence showing the[] policies are an unnecessary or unjustified response to problems of jail security").

227. *King*, 569 U.S. at 464 ("[T]he processing of respondent's DNA sample's 13 CODIS loci did not intrude on respondent's privacy in a way that would make his DNA identification unconstitutional.").

228. *Id.* at 464–65. The Maryland statute states, "a person may not willfully test a DNA sample for information that does not relate to the identification of individuals as specified in this subtitle." MD. CODE ANN., PUB. SAFETY § 2-512(c) (LexisNexis 2018).

229. *See supra* notes 184–86 and accompanying text.

creation of and access to a universal database, which of course would include everyone—not just those suspected of or arrested for a crime—was considered to be at least as intrusive as a patdown, perhaps because our participants believed that their own DNA is much more likely to be in such a database.

At the same time, the universal database was considered somewhat less intrusive than police access to more selective databases such as those maintained by DTC-GT companies (especially in the first-person scenario, described in Appendix D), even though the participants' DNA is less likely to be found in the latter location. This distinction suggests that the survey participants are more willing to permit access to a database in which everyone must submit their DNA for the express purpose of assisting law enforcement (the universal database) than to a DTC-GT database that is created for other reasons, that is not mandatory, and that does not include everyone.[230] Again, the situs of the information, rather than the information itself or whether it is voluntarily surrendered, seems to be the driving factor in the intrusiveness ratings.

2. *Public Databases.* The collection question here is easily answered as a doctrinal matter. Collection by public databases like GEDmatch is clearly not governed by the Fourth Amendment, because the DNA is not sought by the government and is submitted voluntarily. Traditional Fourth Amendment doctrine would also permit access to this database, whether openly or through deception, because in either case the consumer has voluntarily surrendered the information to a third party.

Even after *Carpenter*, that may remain the outcome. Again, *Carpenter* gave two basic reasons for its holding. First, as we noted earlier, the Court stated 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."[231] If all the police learn from a company like GEDmatch are the names of matches or partial matches to a crime scene sample, that information is hardly "exhaustive." Admittedly, if the police do not obtain a direct match but only several partial matches

230. *Cf.* Hazel et al., *supra* note 223, at 899 ("[A] universal database would eliminate or reduce problems associated with the current haphazard genetic investigative regime.").

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

and ostentatiously track down each of them, unsought information may be exposed. Most obviously, people who use these services may find out about a relative—say, a half-sibling who is a serial killer—who they would rather never have discovered.[232] But that should be all that they discover. Recall that in *King* the Court was willing to assume that, even if law enforcement agencies obtain a complete DNA sample, much less a profile of the sample, they can be counted on to limit themselves to identification and crime-scene matching, and not use the genetic material for other purposes or to reveal information to other parties unnecessarily.[233] Illustrating that stance, the 2019 DOJ Interim Policy provides that all profiles and related account information "shall be treated as confidential," that genetic testing services should remove genetic information submitted by law enforcement after arrest of a suspect, and that these materials may not be used "to determine the sample donor's genetic predisposition for disease or any other medical condition or psychological trait."[234]

The second reason *Carpenter* gave for its decision is even less applicable in this setting. The reason is worth quoting in full:

> Cell phone location information is not truly "shared" as one normally understands the term . . . . [C]ell 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 . . . . Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[] the risk" of turning over a comprehensive dossier of his physical movements.[235]

DNA samples surrendered to a public database, in contrast, are "truly 'shared,'" because the services GEDmatch provide are not "indispensable to participation in modern society";[236] rather, the consumer can forgo sharing the information without significant hardship. Of course, the partial matches might lead police to people

232. *See, e.g.*, George Doe, *With Genetic Testing, I Gave My Parents the Gift of Divorce*, VOX (Sept. 9, 2014, 7:50 AM), https://www.vox.com/2014/9/9/5975653/with-genetic-testing-i-gave-my-parents-the-gift-of-divorce-23andme [https://perma.cc/4LMP-BSF2].

233. *See King*, 569 U.S. at 464.

234. DOJ INTERIM POLICY, *supra* note 151, at 6–7.

235. *Carpenter*, 138 S. Ct. at 2220 (first quoting Riley v. California, 573 U.S. 373, 385 (2014); then quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

236. *Cf. id.*

who have never even considered submitting their DNA to a database and who may now be subjected to police interviews or attempts to collect their DNA, surreptitiously or through other means.[237] But note that, once the police obtain the name of a partial match, old-fashioned legwork could usually create the same family tree a database company might provide, and that once police get a name, the rules governing police efforts to collect the DNA of these relatives, overtly or covertly, are no different than if access to the database had never occurred. The important fact for third-party doctrine purposes would seem to be that the DNA in the database was voluntarily submitted, which undercuts *Carpenter*'s importance in this context.

Yet our survey participants viewed the scenario based on the use of GEDmatch in the GSK case to be more intrusive than government access to the cell-site location data at issue in *Carpenter*,[238] suggesting that they do not consider the voluntariness of the interaction with the third party to be relevant. In contrast, recall that the familial matching scenario in our survey involved a *forensic* database, which obtains samples *involuntarily*, was rated toward the bottom of the intrusiveness hierarchy, even though concerns about undiscovered relatives of the type discussed above are equally apposite there. Thus, in evaluating the GEDmatch-type scenario, our participants seemed to be focused on the type of database at issue and perhaps also the fact that the police are engaging in deception in obtaining the match—a concern the new DOJ policy, which generally bars the type of police action used in the GSK case,[239] appears to endorse. To our subjects, those criteria appear to be more relevant to privacy interests than whether information is

237. *See supra* notes 88–99 and accompanying text.

238. Technically, cell-site location data might be less precise than cell-phone location data using GPS signals. *See Carpenter*, 138 S. Ct. at 2218 (noting that the cell-site data only "placed [the subject] within a wedge-shaped sector ranging from one-eighth to four square miles"); Douglas Starr, *What Your Cell Phone Can't Tell the Police*, NEW YORKER (June 26, 2014), https://www.newyorker.com/news/news-desk/what-your-cell-phone-cant-tell-the-police [https://perma.cc/JLH8-NY8B] (describing the uncertainties of cell-site location data). Our survey referred to "cell-phone location data from the[] cell phone company," *infra* Appendix A, which, although accurately describing the cell-site location data in *Carpenter*, could also be influenced by participants' familiarity with the pinpoint accuracy of GPS location data, *cf.* J. Clement, *Most Popular Mapping Apps in the United States as of April 2018, by Monthly Users*, STATISTICA (Nov. 20, 2019), https://www.statista.com/statistics/865413/most-popular-us-mapping-apps-ranked-by-audience [https://perma.cc/9FRY-LJPW] (reporting over 220 million monthly users of iOS mapping apps in the United States alone).

239. DOJ INTERIM POLICY, *supra* note 151, at 6.

voluntarily shared with a third party or whether a police investigation might expose a family tree.

3. *Private Databases.* The collection question here is again easily answered because the government is not involved at this stage. The access question is harder to answer as a doctrinal matter, however. Unlike with public databases, the average consumer assumes the DNA sample and the profile will be kept private, at least in identified form, unless and until the consumer decides to reveal it.[240] At the same time, *Carpenter* suggests that such access is not a search because, as with the public database scenario, providing one's DNA sample to a DTC-GT company is not a crucial aspect of participating in society.

Again, however, our survey participants do not appear to care about this latter point. They rate government access to DTC-GT databases as more intrusive than fraudulent access to a public database and on a par with access to bedrooms and emails, which requires a warrant, as well as on a par with access to financial records, which arguably should require one. Here, the private nature of the database produces a result that suggests the Fourth Amendment is implicated in full force.

4. *Research-Oriented Databases.* Research databases may be maintained by a variety of third parties, such as health care providers, researchers, or DTC-GT companies. The collection issue here is muddied to some extent if the government is sponsoring the collection, as occurs with the *AoU* Research Program. But the collection is still voluntary and is not for law enforcement purposes, so the Fourth Amendment probably would not apply. Nor would it likely govern police access to research-based databases, since once again, the information is voluntarily surrendered in the sense meant by *Carpenter*. But here, it is the *government* that is guaranteeing that the genetic information will be used only for a specific, non-law enforcement purpose, which might give courts more pause.

In any event, our participants viewed accessing this type of database as similar in intrusiveness to police accessing public and

240. *See* Emily Christofides & Kieran O'Doherty, *Company Disclosure and Consumer Perceptions of the Privacy Implications of Direct-to-Consumer Genetic Testing*, 35 NEW GENETICS & SOC'Y 101, 114–16 (2016) (reporting on a survey of consumers of DTC-GT designed to evaluate their understanding of privacy information and expected uses of information and samples).

private databases and as more intrusive than accessing a government-run database. Again, the type of database, not its precise contents, seems to be driving the results.

CONCLUSION

Overall, our findings suggest that members of society asked to differentiate government attempts to obtain genetic information use different metrics than the courts. At least when DNA is accessed solely for the purpose of matching a person with a crime, the extent to which people associate genetic information with privacy significantly depends on where it is located, not its content or whether it was "voluntarily" surrendered. Thus, according to our results, DNA given to one's doctor for analysis is more closely associated with privacy than DNA given to a publicly accessible genealogy service, a private DTC-GT company, or a government-sponsored research entity. And, from the perspective of our survey participants, all of these scenarios are more entitled to privacy than the DNA *in*voluntarily provided to an arrestee-based database or unknowingly discarded DNA found in public. Similarly, our findings suggest that when DNA is maintained in places akin to the home, it is entitled to maximum privacy protection. Specifically, when DNA is found in a doctor's office or a private or public database, police access to it is perceived to be similar in intrusiveness to searches of bedrooms, emails, and texts.[241] Those outcomes are consonant with Justice John Marshall Harlan's observation in *Katz* that although "'the Fourth Amendment protects people, not places[,]' . . . what protection it affords to those people generally "requires reference to a 'place.'"[242]

Yet, despite our findings, at present none of these genetic storage places are clearly protected against government access by the Fourth Amendment, much less the warrant requirement. We think the Court should reconsider that position. Our results, if replicated, suggest that contrary to the dictates of the third-party doctrine, the Fourth Amendment should govern whenever law enforcement seeks access to genetic information held in medical records or in private, public, or research genetic databases. Further, given that searches of bedrooms, emails, and texts require a warrant, a warrant should be required for

241. *See, e.g.*, *supra* Table 1 (ranking searches of bedrooms, text messages, DNA databases, and emails within a spread of 2 points on a 100-point scale).

242. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (quoting *id.* at 351 (majority opinion)).

these types of government searches as well, whether conducted overtly or covertly.[243]

Such a warrant would not be easy to obtain under traditional rules requiring probable cause to believe evidence will be found in a particularized location.[244] Police would have to make two probable cause showings: (1) that they have an identified suspect or the DNA of a suspect from a crime scene; and (2) that the suspect's DNA, or a full or partial match to the crime scene DNA, will be discovered in the targeted database.[245] The first showing will usually be straightforward, although problems can arise with respect to match inquiries if police cannot clearly show that the crime-scene DNA comes from the perpetrator. The second showing will be much more difficult, given the likelihood police will have no idea which, if any, databases might contain the DNA of the suspect or a family member. However, such a showing might be possible if, based on the type of research we described earlier, the Court is willing to find that probable cause exists because, given the size of many of the databases that law enforcement is likely to target, there is a significant probability that virtually anyone is likely to have at least one relative in the database.[246]

An analogy to this latter scenario comes from a recent judicial development in the realm of electronic information called the "reverse location warrant." In the reverse warrants granted to date, police have successfully compelled telecommunications companies to disclose cell-location information about all phones near a crime scene at the time the crime occurred—information which then might be used to track down suspects or witnesses through various means, including warrant-based inquiries into their communications.[247] The rationale for such

243. If one follows the results in Table 1 regarding forensic databases, a warrant might also be required for government access to its own databases, the content of which should be limited to collection of DNA from those arrested for serious crimes.

244. *See generally* CHARLES H. WHITEBREAD & CHRISTOPHER SLOBOGIN, CRIMINAL PROCEDURE: AN ANALYSIS OF CASES AND CONCEPTS ch. 5 (7th ed. 2020) (describing the probable cause and particularity requirements of the Warrant Clause of the Fourth Amendment).

245. The Fourth Amendment requires probable cause to believe that the items sought will be found in the place to be searched. *See* Steagald v. United States, 451 U.S. 204, 214 n.7 (1981) ("[A]bsent exigent circumstances the magistrate, rather than the police officer, must make the decision that probable cause exists to believe that the person or object to be seized is within a particular place.").

246. *See* Erlich et al., *supra* note 17, at 690.

247. *See, e.g.*, Aaron Mak, *Close Enough*, SLATE (Feb. 19, 2019, 5:55 AM), https://slate.com/technology/2019/02/reverse-location-search-warrants-google-police.html [https://perma.cc/JZ5S-

authorizations is that only one fact about the individuals identified in this manner is discovered: where they were at a particular time.[248] Warrants limiting police to familial searches using public and private databases might be justified on similar grounds, since all that will be discovered is a match or partial genetic match. Given the smaller number and large size of common carriers, the probability that a particular communications company will have the relevant information may be higher in the reverse-warrant situation than in the genetic setting. But as DTC-GT and public databases grow and familial matching techniques improve, that difference is decreasing. Commentators have correctly raised concerns about the broad scope of reverse cell-location warrants.[249] But such a regime, applied to genetic data and familial searches, would provide sufficiently more oversight of these activities than the existing system.

Our research also suggests that the Fourth Amendment should govern when the police obtain a partial match through the process just described and then want to obtain the DNA of relatives of the partial match *covertly* rather than consensually. As indicated in Table 1, our subjects ranked covert collection as relatively low in intrusiveness, which suggests a traditional warrant should not be required in this situation. However, this scenario was still routinely ranked as more intrusive than a roadblock, which requires some sort of suspicion when it is aimed at detecting ordinary crime. As applied to covert DNA collection, this reasoning suggests that, before engaging in covert DNA collection, police should have to explain to a judge—ideally, before the collection takes place—how they have narrowed the pool of relatives from whom DNA is sought and why there is good reason to believe that those who remain in the pool could be a direct match. The Supreme Court case most on point in this regard is *Illinois v. Lidster*,[250] which upheld a roadblock established at the same time and place as a

CFN3]. For a review of cases that have addressed this issue, see generally Donna Lee Elm, *Geofence Warrants: Challenging Digital Dragnets*, 35 CRIM. JUST. 7 (2020).

248. *See, e.g.*, United States v. Walker, No. 18-CR-37, 2020 WL 4065980, at *8 (E.D.N.C. July 20, 2020) ("[T]he privacy concerns underpinning the court's holding in *Carpenter* do not come into play . . . where the search for data focuses not on 'the whole of [an individual's] physical movements' but rather on the data that was left behind at a particular time and place by virtue of cell phone tower locations." (second alteration in original) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018))).

249. *See* Elm, *supra* note 247, at 9–12; Daniel K. Gelb, *Is the Reverse Location Search Warrant Heading in the Wrong Direction?*, 34 CRIM. JUST. 68 *passim* (2019).

250. Illinois v. Lidster, 540 U.S. 419 (2004).

hit-and-run accident that occurred a week earlier, in an effort to identify eyewitnesses to, or the perpetrator of, the accident.[251] The Court stated that the analysis in such cases should consider "the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty."[252] A formulation along these lines should also govern covert DNA collection if the results of our study are given weight in the analysis.

One might disparage this suggested regulatory regime on the grounds that survey results, even if solidly representative of public views, are not relevant to Fourth Amendment questions, and that a balancing analysis, property law, or some other judicial metric should dictate the amendment's scope.[253] But there are several reasons to reject this view, the first two of which were noted earlier.[254] First, the Supreme Court's own formulation of the Fourth Amendment's scope references expectations of privacy "recognized by society." The plain meaning of this language calls for an assessment of the public's views. Second, privacy is ultimately dependent on societal mores, which can only be ascertained through some sort of empirical assessment. Indeed, survey results, with all of their flaws, can provide stability to an area of the law that, to date, has relied mostly on judicial intuitions about privacy or property.[255]

Third, there are real-world effects of a Fourth Amendment regime that ignores the public's views. As Kugler and Strahilevitz have pointed out:

> When there is a sharp divide between what the courts describe as the Fourth Amendment's scope and what the people actually expect the Fourth Amendment's scope to be, various problems arise. Law-abiding people may take excessive precautions to protect their

---

251. *Id.* at 427–28.

252. *Id.* at 427 (quoting Brown v. Texas, 443 U.S. 47, 51 (1979)).

253. *See generally* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007) (describing both normative and descriptive models of Fourth Amendment protection).

254. *See supra* notes 39–41 and accompanying text.

255. *See* Minnesota v. Carter, 525 U.S 83, 97 (1998) (Scalia, J., concurring) ("[T]he only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, those 'actual (subjective) expectation[s] of privacy' 'that society is prepared to recognize as "reasonable"' bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable." (second alteration in original) (citation omitted) (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring))).

> information, keeping it not only from the state's agents but also from third parties who could put the information to productive uses. Or citizens might make inordinate investments in learning the contours of Fourth Amendment law, time and money that could be better spent elsewhere. Also, mistaken expectations limit the effectiveness of the democratic process as a check on law enforcement surveillance; the public may not move legislatively to protect privacy if they mistakenly believe it is already protected constitutionally. Disconnects between actual law and perceived law may also provide police officers and prosecutors with undue leverage over citizens.[256]

Finally, if the courts depart substantially from societal mores, their own legitimacy—not just the legitimacy of the practices they condone—could suffer.[257] *Carpenter* seemed to recognize that possibility: "Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone."[258] Today, with the combination of government, private, and public DNA databases now in existence, the government's "newfound tracking capacity" to identify people's genetic markers "runs against [almost] everyone."[259] Recall the hypothetical that began this Article. If the Justices announced that the third-party or knowing-exposure doctrines applied to every step the police in that case took to obtain DNA—in effect, shielding these activities from Fourth Amendment scrutiny—the Court would likely do serious damage to its prestige and authority. Research like that reported in this Article can help the courts gauge how far they should go in contracting or expanding Fourth Amendment rights.

---

256. Kugler & Strahilevitz, *supra* note 194, at 227 (footnote omitted).

257. SLOBOGIN, *supra* note 41, at 116; *see also* Heather Murphy, *Playing Catch a Killer with a Room Full of Sleuths*, N.Y. TIMES (Dec. 30, 2019), https://nyti.ms/2VdgOG7 [https://perma.cc/8M7A-KBZ6] (quoting Diahan Southard, an instructor at a program training law enforcement officers about genetic searches, as warning that continued availability of such searches "depends on having the support of regular people . . . . If you can't convince the public that it's safe, it's going to go away").

258. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

259. *Cf. id.*

APPENDIX A: FULL TEXT OF STUDY SCENARIOS

Genetic Data Focused	
Search for Suspect in Forensic DNA DB	Police searching a law enforcement DNA database that contains the DNA profiles of people who have been arrested: they want to see if they can find a match between an unknown DNA sample and a person in the database.
Familial Search of Forensic DNA DB	Police uploading a person's DNA profile (found at a crime scene) to a law enforcement database that contains the DNA profiles of people who have been arrested, in the hope that they will find a match with either the person or one of their relatives who can help identify them.
Compelled DNA Collection from Arrestees	Police collecting a DNA sample from a person after they have been arrested for a crime as part of the normal "booking" process.
Collection for a Universal DNA DB	Police collecting a DNA sample from everyone, at birth or upon entry to the country as a visitor, to create a nationwide law enforcement database.
Genetic Data from DTC-GT Company	Police getting a person's DNA profile from a genetic testing company (for example, Ancestry.com or 23andMe) that the person had used in the past.
Genetic Data from Doctor	Police getting a person's DNA profile from their doctor.
Genetic Data from Researchers	Police getting a person's DNA profile from a research study that the person had been a part of.

Familial Search of Public Genealogy DNA DB	A police officer uploading a person's DNA profile (found at a crime scene) to a publicly accessible genealogy DNA database, pretending the DNA is theirs, in the hope that they will find a match with either the person or with a relative of the person who can help identify them.
Surreptitious Collection of Discarded DNA	Police collecting an item that a person has thrown away, like a used soda can or cigarette, and creating a DNA profile from it.
Other Data Types and Searches	
Medical Records	Police getting a person's medical records from their doctor.
Text Messages	Police looking at all of the text messages that a person has sent or received on their phone.
Emails	Police looking at all of the emails that a person has sent or received on their computer.
Phone Numbers	Police getting a list of all the phone numbers that a person has received calls from or placed calls to from their telephone company.
Social Media	Police looking at a person's social media profile and posts (for example, on Facebook); the profile and posts are not visible to the public.
Web History	Police getting a list of all the websites that a person has visited from their internet service provider.
Cell Location	Police getting a person's cell phone location data from their cell phone company.
Financial Records	Police getting a person's financial records from their bank.

Universal Fingerprint DB	Police collecting the fingerprints of everyone to create a nationwide law enforcement database.
Bedroom Search	Police searching a person's bedroom.
Pat Down	Police patting-down a person's clothing during a brief stop.
Roadblock	Police stopping people at a roadblock.

APPENDIX B: SURVEY VARIATIONS (EXPERIMENTAL MANIPULATIONS)

Third Person (Baseline Survey):

In the baseline survey, participants were given the following instructions and assumptions:

Instructions:
You will be presented with 21 scenarios involving actions by police.

Assume in each scenario that:
1) the police are looking for evidence of some type of criminal activity; but that
2) the person is presumed innocent of any criminal wrongdoing; and that
3) the person did not consent to the police action.

First-Person Variation:

- Assumptions 2 & 3 were modified to read: "2) you are presumed innocent of any criminal wrongdoing; and "3) you did not consent to the police action".
- All 21 scenarios were presented in the first person (e.g. "police obtaining your DNA profile . . ." as opposed to "a person's DNA profile . . .").

Serious-Crime Variation:

- Assumption 1 was modified to read: "the police are looking for evidence that could help solve a serious crime that has been

committed (such as murder, sexual assault, or terrorism); but that . . .”

Prevent-Serious-Crime Variation:

- Assumption 1 was modified to read: “the police are looking for evidence that could help prevent a serious crime from being committed (such as murder, sexual assault, or terrorism); but that . . .”

Hindsight-Bias Variation:

- As in the Serious Crime variation, Assumption 1 was modified to read: “the police are looking for evidence that could help solve a serious crime that has been committed (such as murder, sexual assault, or terrorism); but that . . .”
- The following additional Assumption was also added after Assumption 1: “the police found evidence of criminal activity by the person; but that . . .”

APPENDIX C: DEMOGRAPHICS OF STUDY POPULATION

Demographic	**Group**	**n**	**%**
Race	American Indian or Alaska Native	22	1.4%
	Asian	79	4.9%
	Black or African American	180	11.3%
	Middle Eastern or North African	1	0.1%
	Native Hawaiian or other Pacific Islander	1	0.1%
	White	1257	78.7%
	None of these fully describe me	39	2.4%
	Prefer not to answer/No response	18	1.1%

Hispanic, Latino, or Spanish Origin	Yes	172	10.8%
	No	1391	87.5%
	Prefer not to answer/No response	34	1.7%
Gender	Female	735	46.0%
	Male	845	52.9%
	Other/Prefer to self-describe	6	0.4%
	Prefer not to answer/No response	11	0.7%
Marital Status	Single	738	46.2%
	Married	723	45.3%
	Divorced	95	5.9%
	Separated	23	1.4%
	Prefer not to answer/No response	18	1.1%
Age	18 to 29	450	28.2%
	30 to 44	770	48.2%
	45 to 59	269	16.8%
	60 and over	63	3.9%
	Prefer not to answer/No response	45	2.8%
Sexual Orientation	Straight/Heterosexual	1363	85.3%
	Gay or Lesbian	48	3.0%
	Bisexual	152	9.5%
	Other/Prefer to self-describe	12	0.8%

	Prefer not to answer/No response	22	1.4%
Education	Less than a high school degree	3	0.2%
	High school graduate, GED	165	10.3%
	Some college credit, no degree	327	20.5%
	Trade/technical/vocational training	61	3.8%
	Associate degree	195	12.2%
	Bachelor's degree	648	40.6%
	Graduate or Professional degree	186	11.6%
	Prefer not to answer/No response	12	0.8%
Income	Less than $20,000	255	16.0%
	$20,000 to $34,999	314	19.7%
	$35,000 to $49,999	321	20.1%
	$50,000 to $74,999	368	23.0%
	$75,000 to $99,999	180	11.3%
	$100,000 to $149,999	88	5.5%
	$150,000 to $199,999	22	1.4%
	$200,000 or more	12	0.8%
	Prefer not to answer/No response	37	2.3%
Political Affiliation	Republican	322	20.2%
	Leans Republican	137	8.6%
	Independent	350	21.9%

	Leans Democrat	250	15.7%
	Democrat	508	31.8%
	Prefer not to answer/No response	30	1.9%
Interactions with Law Enforcement	All positive	362	22.7%
	Mostly positive	629	39.4%
	Both positive and negative	354	22.2%
	Mostly negative	122	7.6%
	All negative	30	1.9%
	No previous interactions	78	4.9%
	Prefer not to answer/No response	22	1.4%
Type of Neighborhood	High crime neighborhood	42	2.6%
	Moderate crime neighborhood	316	19.8%
	Low crime neighborhood	1148	71.9%
	I don't know	69	4.3%
	Prefer not to answer/No response	22	1.4%
Previous Genetic Testing? *(check all that apply)*	Doctor-Ordered	143	9.0%
	Direct-to-Consumer	185	11.6%
	For Research	92	5.8%
	Unsure	75	4.7%
	No	1177	73.7%
	Prefer not to answer/No response	58	3.6%

APPENDIX D: EFFECT OF EXPERIMENTAL MANIPULATIONS

TABLE 2: FIRST PERSON SURVEY VARIATION: INTRUSIVENESS AND EXPECTATIONS OF PRIVACY FOR 21 SCENARIOS

Perspective: 1st Person (*n = 313*)		**Intrusiveness**			**REP?**
#	**Scenario:**	**Mean**	**Z**	**S.D.**	**% Yes**
1	Bedroom Search*†	83.2	± 2.2	19.9	82.1%
2	Genetic Data from Doctor*	82.0	± 2.4	21.8	89.1%
3	Text Messages*	80.7	± 2.1	19.2	81.5%
4	Medical Records*†	80.4	± 2.5	22.9	88.8%
5	Emails*†	79.3	± 2.3	20.4	84.7%
6	Financial Records*†	77.8	± 2.4	21.8	84.0%
7	Genetic Data from DTC-GT Company†	75.3	± 2.9	25.8	82.7%
8	Genetic Data from Researchers*	74.8	± 2.9	25.8	82.7%
9	Web History*†	74.1	± 2.5	22.7	79.6%
10	Familial Search of Public Genealogy DNA DB†	74.0	± 3.1	27.8	77.6%
11	Phone Numbers*	70.0	± 2.6	23.2	75.1%
12	Cell Location*	69.0	± 2.7	24.2	69.3%
13	Collection for a Universal DNA DB	68.6	± 3.3	30.1	69.0%
14	Social Media*†	68.5	± 2.9	25.9	74.1%
15	Pat Down	59.1	± 3.1	27.7	40.9%
16	Universal Fingerprint DB	58.6	± 3.4	31.1	57.5%
17	Surreptitious Collection of Discarded DNA*	57.1	± 3.3	29.6	49.2%
18	Compelled DNA Collection from Arrestees	50.5	± 3.5	31.2	37.7%
19	Familial Search of Forensic DNA DB*†	49.1	± 3.3	29.9	43.5%

20	Search for Suspect in Forensic DNA DB*	41.9	± 3.4	31.0	36.7%
21	Roadblock	35.2	± 2.9	26.0	20.1%

Symbols indicate scenarios where a statistically significant ($p \leq 0.05$) *increase* in mean intrusiveness (*) and/or expectation of privacy (†) was observed when compared to the baseline survey (Table 1).

TABLE 3: SERIOUS CRIME SURVEY VARIATION: INTRUSIVENESS AND EXPECTATIONS OF PRIVACY FOR 21 SCENARIOS

Serious Crime (*n = 319*)		**Intrusiveness**			**REP?**
#	**Scenario:**	**Mean**	**Z**	**S.D.**	**% Yes**
1	Genetic Data from Doctor	76.2	± 2.6	24.1	83.1%
2	Medical Records	73.5	± 2.6	23.3	85.6%
3	Collection for a Universal DNA DB†	73.2	± 3.2	29.6	74.3%
4	Bedroom Search	72.8	± 2.5	22.6	71.2%
5	Familial Search of Public Genealogy DNA DB	71.7	± 3.2	29.2	70.5%
6	Emails	70.8	± 2.5	23.2	71.2%
7	Genetic Data from DTC-GT Company	70.6	± 2.9	26.7	77.1%
8	Financial Records	70.3	± 2.6	23.8	76.2%
9	Text Messages	70.2	± 2.5	23.2	74.9%
10	Genetic Data from Researchers	69.6	± 2.9	26.9	74.6%
11	Web History	66.4	± 2.7	25.0	67.4%
12	Universal Fingerprint DB	64.9	± 3.5	32.1	63.6%
13	Phone Numbers	61.2	± 2.8	25.4	63.6%
14	Social Media	59.3	± 3.0	27.2	61.4%
15	Cell Location	59.0	± 2.8	25.9	61.8%

16	Pat Down	52.9	± 3.0	27.2	40.4%
17	Compelled DNA Collection from Arrestees	48.6	± 3.3	29.9	36.4%
18	Surreptitious Collection of Discarded DNA	47.7	± 3.4	30.7	40.1%
19	Roadblock	40.7	± 3.2	29.2	27.0%
20	Familial Search of Forensic DNA DB	39.4	± 3.5	32.0	30.1%
21	Search for Suspect in Forensic DNA DB	30.8	± 3.3	30.0	23.8%

Symbols indicate scenarios where a statistically significant ($p \leq 0.05$) *increase* in mean intrusiveness (*) and/or expectation of privacy (†) was observed when compared to the baseline survey (Table 1).

TABLE 4. PREVENTION OF SERIOUS CRIME SURVEY VARIATION: INTRUSIVENESS AND EXPECTATIONS OF PRIVACY FOR 21 SCENARIOS

Objective: Prevent Serious Crime (*n = 318*)		**Intrusiveness**			**REP?**
#	**Scenario:**	**Mean**	**Z**	**S.D.**	**% Yes**
1	Genetic Data from Doctor	78.8	± 2.6	23.2	84.3%
2	Medical Records	75.9	± 2.5	22.5	85.2%
3	Collection for a Universal DNA DB	73.5	± 3.2	29.2	73.0%
4	Bedroom Search	72.0	± 2.8	25.8	76.7%
5	Genetic Data from DTC-GT Company	71.6	± 2.9	26.5	80.8%
6	Familial Search of Public Genealogy DNA DB	70.6	± 3.2	29.3	73.0%
7	Financial Records	70.6	± 2.6	23.7	79.6%
8	Genetic Data from Researchers	70.1	± 2.9	26.8	79.9%
9	Emails†	70.0	± 2.7	24.6	78.6%
10	Text Messages	69.8	± 2.8	25.3	79.6%

11	Web History†	67.2	± 2.8	25.3	75.8%
12	Phone Numbers†	63.2	± 2.7	24.2	72.3%
13	Universal Fingerprint DB	63.1	± 3.7	33.5	65.7%
14	Social Media	59.8	± 3.1	27.9	67.3%
15	Cell Location	58.7	± 3.0	26.9	68.6%
16	Pat Down	54.0	± 3.0	27.2	39.3%
17	Compelled DNA Collection from Arrestees	48.8	± 3.5	31.8	36.2%
18	Surreptitious Collection of Discarded DNA	46.6	± 3.3	29.9	45.6%
19	Roadblock	40.1	± 3.4	30.5	26.1%
20	Familial Search of Forensic DNA DB†	38.7	± 3.3	30.1	38.4%
21	Search for Suspect in Forensic DNA DB†	31.8	± 3.3	29.7	31.4%

Symbols indicate scenarios where a statistically significant ($p \leq 0.05$) *increase* in mean intrusiveness (*) and/or expectation of privacy (†) was observed when compared to the serious crime variation of the survey (Appendix D, Table 2).

TABLE 5. HINDSIGHT BIAS SURVEY VARIATION: INTRUSIVENESS AND EXPECTATIONS OF PRIVACY FOR 21 SCENARIOS.

Hindsight Bias (Evidence Found) (*n = 324*)		**Intrusiveness**			**REP?**
#	**Scenario:**	**Mean**	**Z**	**S.D.**	**% Yes**
1	Genetic Data from Doctor	75.2	± 2.8	25.3	84.3%
2	Medical Records	73.6	± 2.6	23.7	81.2%
3	Collection for a Universal DNA DB	71.5	± 3.2	29.3	74.4%
4	Familial Search of Public Genealogy DNA DB	70.2	± 3.1	28.5	72.5%
5	Bedroom Search*	68.3	± 2.7	25.2	65.4%
6	Genetic Data from DTC-GT Company	67.9	± 2.9	26.8	75.6%

7	Financial Records	67.7	± 2.8	25.6	71.3%
8	Emails	67.4	± 2.7	24.5	67.9%
9	Text Messages†	67.1	± 2.7	25.1	67.6%
10	Genetic Data from Researchers*	63.4	± 3.1	28.8	75.9%
11	Universal Fingerprint DB	63.3	± 3.5	32.3	64.5%
12	Web History*	61.9	± 2.9	27.0	61.1%
13	Phone Numbers	57.9	± 2.8	25.9	59.0%
14	Cell Location	57.6	± 2.9	26.7	56.8%
15	Social Media†	55.4	± 3.1	28.1	53.7%
16	Pat Down	54.8	± 3.0	27.8	41.7%
17	Compelled DNA Collection from Arrestees	44.6	± 3.4	31.1	34.9%
18	Surreptitious Collection of Discarded DNA	43.8	± 3.1	28.9	37.3%
19	Roadblock	42.1	± 3.2	29.6	29.6%
20	Familial Search of Forensic DNA DB	38.2	± 3.3	30.6	30.2%
21	Search for Suspect in Forensic DNA DB	31.3	± 3.2	29.4	26.9%

Symbols indicate scenarios where a statistically significant ($p \leq 0.05$) *decrease* mean intrusiveness (*) and/or expectation of privacy (†) was observed when compared to the serious crime variation of the survey (Appendix D, Table 2).