A Cautionary Note: Genealogy Companies Need to Stop Giving Warrantless DNA Clues to Law Enforcement

Katelyn N. Ringrose[1]

Introduction

***

In 2018, seventy-two-year-old Joseph DeAngelo was accused of committing over one-hundred burglaries, fifty rapes, and thirteen murders that took place throughout California from the mid-1970s to the mid-1980s.[2] DeAngelo has gone by many names during his time as California's most prolific unidentified serial-rapist and murderer. However, the East Area Rapist, Visalia Ransacker, Original Night Stalker, and Golden State Killer all have one crucial thing in common—their DNA.

DeAngelo's DNA, after being housed in a storage locker for decades, was uploaded to the Combined DNA Index System

1. Katelyn Ringrose writes on surveillance, privacy, and tech policy. Katelyn wrote this note under the advisement of Professor Patricia Bellia, and would like to thank the Center for Democracy and Technology, for advice on this note, as well as the Future of Privacy Forum, where she continues her work on genetic privacy. This note is intended to serve as the basis for a conversation between law enforcement, consumer companies, privacy organizations, and legislators regarding law enforcement use of genetic testing services.

2. *See* Amelia Perry, *Golden State Killer Trial: Joseph DeAngelo Case Could Last 10 Years*, ROLLING STONE (Dec. 9, 2018), https://www.msn.com/en-us/news/crime/golden-state-killer-trial-joseph-deangelo-case-could-last-10-years/ar-BBQEcs0 (DeAngelo's case is currently pending trial in California, it is expected to be one of the largest in California history, with an expected budget of around $20 million.).

(CODIS) by local law enforcement in 2000.[3] The FBI designed CODIS to find direct matches, and the bureau enforces a strict criteria for familial searches, with most states disallowing familial matching from taking place on the site at all.[4] With no CODIS match for DeAngelo's DNA, and genealogy websites offering endless possibilities for familial-based cold hits, in 2018, Sacramento law enforcement opted to upload the DNA they had sequenced to GEDmatch. GEDmatch is a third-party site developed to compare data obtained through consumer use of direct-to-consumer genetic testing companies like 23andMe and AnscestryDNA.[5]

The officers did not ask for, nor did they receive a court order, and the limits to the officers' authority are unclear.[6] After DeAngelo's DNA was matched to another DNA sequence belonging to a GEDmatch user, law enforcement directed their attention to male relatives of that individual.[7] After narrowing their sights on DeAngelo, as being of an appropriate age and having shared characteristics with the unidentified offender, law

3. *CODIS*, FBI.GOV, https://www.fbi.gov/services/laboratory/biometric-analysis/codis (last visited Oct. 4, 2019) (While CODIS allows law enforcement agents to search for familial matches, DNA sequences indicating shared genetics between biological families, only certain jurisdictions allow officers to run such searches. California, in particular, disallows familial searching except to compare the DNA of unidentified suspects to the DNA of convicted offenders.).

4. *Id*. In particular, CODIS limits the types of crimes eligible for searching, asks that all other investigative leads first be exhausted, only allows for the DNA of suspected or convicted criminals to be uploaded, and requires approval when it comes to laboratory management. No such requirements are placed on law enforcement seeking to compare an unidentified suspect's DNA on direct-to-consumer genetic testing websites.

5. *Terms of Service and Privacy Policy*, GEDMATCH.COM (May 18, 2019), https://www.gedmatch.com/tos.htm.

6. *Supra* note 2, front page, GEDMATCH.COM, https://www.gedmatch.com/login1.php (According to GEDMatch's front page, the company "provides DNA and genealogical analysis tools for amateur and professional researchers and genealogists." GEDmatch does not mention the capability for law enforcement to trawl its site, except a vague mention on its privacy policy which states that, "when you upload Raw DNA" you agree that it is "DNA obtained and authorized by law enforcement" to "identify a perpetrator of a violent crime against another individual." The website goes on to explain that its definition of a violent crime includes homicides or sexual assaults.).

7. *Supra* note 2.

enforcement harvested an abandoned item of DeAngelo's that contained his DNA. The officers matched his abandoned DNA to the DNA they had on file, unmasking DeAngelo one final time.[8]

DNA is the most personally identifying information ("PII") possible. While other biometrics like facial and iris recognition are increasing in technological accuracy, and fingerprints hold a 98.6% match propensity, DNA, when tested at a high loci point, can yield a near-perfect match. Furthermore, the propensity of DNA as an identifier is almost unending, with its capacity to identify relatives: both living and dead. Some 26 million people have uploaded their DNA to direct-to-consumer genetic testing websites. Researchers conclude that it is nearly possible for every American to be identified through familial matching today, with more matches being accrued over time.[9] There has been increased pressure, especially since DeAngelo's arrest, to utilize genetic testing sites to achieve cold hits, and there have been at least four cold murder cases and one recent rape case solved through similar efforts.[10] The capacity of DNA identification is vast, with admittedly numerous positive benefits, but the practice also holds incredibly harmful implications on privacy. Despite the possibility for abuse, direct-to-consumer ("DTC") genetic-testing companies have been slow to adopt stringent privacy policies adopting best practices when it comes to protecting their consumer's genetic information from law enforcement.[11]

8. *Supra* note 2.

9. Jessica Bursztynsky, *More than 26 Million People shared their DNA with Ancestry Firms, Allowing Researchers to Trace Relationships between Virtually all Americans*, CNBC: HEALTH TECH MATTERS (Feb. 12, 2019, 2:31 PM), https://www.cnbc.com/2019/02/12/privacy-concerns-rise-as-26-million-share-dna-with-ancestry-firms.html.

10. Christi Guerinni et. al, *Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and other Criminals Using the Controversial New Technique*, PLOS BIOLOGY (Oct. 2, 2018), https://www.researchgate.net/publication/328038448_Should_police_have_access_to_genetic_genealogy_databases_Capturing_the_Golden_State_Killer_and_other_criminals_using_a_controversial_new_forensic_technique.

11. Future of Privacy Forum, *Privacy Best Practices for Consumer Genetic Testing Services* (July 31, 2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf (Best practices have been written about in regard to the propensity of sites to transmit information to third-parties, such as insurance or drug companies, but little has been said about the best practices as relates to interactions with law enforcement.).

This note surveys genetic testing companies and examines the current state and federal regulatory landscape, along with issues regarding law enforcement's use of such sites, and the current need for enhanced oversight. In Part I, this note scrutinizes how law enforcement has become privy to genetic information from DTC sites, including so-called public genealogical databases, and whether such searches are constitutional. This note looks into the expectation of privacy Americans reasonably hold in their genetic material.[12] This note also questions whether third-parties, individuals who have voluntarily submitted their DNA, should have a differing expectation of privacy in their genetic material than fourth-parties, individuals whose DNA is only a familial match to that third-party consumer. In Part II, this note examines potential applications of *Carpenter v. United States* to the issue of genetic privacy, and looks to how district courts have been approaching third-party data collection over this past year.[13] HIPAA and GINA, federal laws governing medical data, as well as other medical regulatory mechanisms do not apply to the issue of commercial genetic data. In Part III, this note examines current DTC genetic-testing privacy agreements and finds areas where such policies may be strengthened. In Part IV, this note scrutinizes current law enforcement policies regarding the utilization of DTC websites. If law enforcement is operating in violation with current privacy policies, consumer safeguards need to be updated in order to provide greater protections. Finally, in Part V, this note concludes with a model privacy policy for DTC genetic testing companies, a model state law regarding genetic searches, as well as a model advisory memorandum for law enforcement. This note argues that Americans hold a reasonable expectation of privacy in their DNA, and law enforcement should seek a warrant[14] to gather information from

12. Jennifer King, *Privacy, Disclosure, and Social Exchange Theory* (2018) (unpublished Ph.D. dissertation, University of California, Berkeley), http://www.jenking.net/files/jennifer_king_dissertation_final.pdf.

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

14. Legal processes that law enforcement can currently use can include subpoenas, warrants, or even 2703(d) orders as genetic data has not yet been found to constitute content under the Stored Communications Act or the Electronic Privacy Act. *See* Justice Information Sharing, *SCA and ECPA,* https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last updated Apr. 24, 2019). Genetic data is woefully under-protected. There is some argument to be made that genetic information is, at the least, protected under FOIA when it comes to the confidentiality of genetic materials. *See Best Practices for*

DTC genetic-companies.[15] DTC companies should enhance their lax privacy policies in order to help protect their consumers from third-party intrusions and, what could be, the most invasive law enforcement scheme to date—genetic surveillance.

The Rise of DTC Companies

***

As interest in genetics and genomics has increased, there has been corresponding growth in direct-to-consumer genetic testing sales.[16] There is tremendous diversity when it comes to the types of tests offered by DTCs, as well as a plethora of information available about their services and the practices of each company. Before discussing law enforcement's utilization of DTC websites, it is important to note why DTCs are both so popular and so controversial within the United States.[17]

Critics of DTC genetic testing are often concerned with the quality of the tests, the accuracy and adequacy of the information provided by companies, and the risk that consumers may be misled by false claims. There is also the risk that consumers may make harmful healthcare decisions on the basis of faulty health-related test results. Some critics have asserted that genetic testing should take place only through a healthcare provider and with adequate counseling.[18] Others argue that there are ethical implications of DTC

Consumer Genetic Testing Companies, Future of Privacy Forum 1, 8, (July 31. 2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf.

15. Law enforcement here can include genetic crime solvers, who are individuals hired as independent contractors for purposes of searching through genealogical databases. The Supreme Court recently held in *Carpenter v. United States* that law enforcement need to obtain warrants in order to gain historical cell-site information location (CSLI) from cell-phone carriers. The Court noted that obtaining records from third-parties as to the location of cell phone users violates their expectation of privacy, and that expectation is one that society was prepared to recognize as reasonable. A search of such private information required a warrant supported by probable cause.

16. Erica Ramos & Scott M. Weissman, *The Dawn of Consumer-Directed Testing*, 178 AM J. MED. GENETICS PART C SEMINAR MED. GENETICS XX, 89–97 (2018), https://doi.org/10.1002/ajmg.c.31603.

17. *See* Jennifer K. Wagner et al., *Tilting at Windmills no Longer: a Data-driven Discussion of DTC DNA Ancestry Test*. 14 GENETICS IN MED. 586, 586–593 (2012), https://www.nature.com/articles/gim201177.

18. Stuart Hogarth et al., *The Current Landscape for Direct-to-Consumer Genetic Testing: Legal, Ethical, and Policy Issues*, 9 ANN. REV.

testing that are yet unrealized. Current knowledge and understanding of personal genomics is far from complete, and ancestry data changes over time as datasets grow more expansive. Many genetic markers have not yet been discovered and their contribution to the incidence of disease, as well as their interaction with one another, is not clear, making the clinical application of such tests rather limited. Furthermore, the implications of what we do know, but do not fully comprehend, on disease prevention or treatment has yet to be determined.[19] Individuals concerned about the ethical bounds of genetic testing point to this lack of knowledge to be quite disturbing, as consumers often take the results of DTC tests quite seriously. Over the past few years, ethical considerations abound concerning the capacity of such genetic testing to influence things like access to health insurance.[20] There are also concerns about which companies are profiting from the monetization of genetic data.[21] While this paper looks to concerns surrounding law enforcement's use of such technologies, it is important to keep other issues at the forefront of conversations revolving around genetic testing.

Conversely, advocates of DTC testing—generally purveyors of genetic tests—contend that DTCs provide numerous positive benefits. Such tests can help improve health and help allow consumers to make beneficial treatment and lifestyle decisions.[22] These groups also claim that DTC testing provides a privacy advantage over testing through a healthcare provider. There are also advocates that believe in the use of DTC websites by law enforcement. Individuals argue that DTC sites have the unparalleled ability to identify individuals like the Golden State Killer, and bring relief to victims' families. From a privacy standpoint, proponents argue that they have nothing to hide from law enforcement, and

GENOMICS HUM. GENETICS 161, 161–82 (2008), http://www.cienciaviva.eu/projectos/2ways/artigo1.pdf.

19. Laurie Udesky, *The Ethics of Direct-to-Consumer Genetic Testing*, 376 THE LANCET 1377, 13771–78 (Oct. 23, 2010), https://doi.org/10.1016/S0140-6736(10)61939-3.

20. Mark Hall & Stephen Rich, *Laws Restricting Health Insurers' Use of Genetic Information: Impact on Genetic Discrimination*, 66 AM. J. OF HUM. GENETICS 293, 2931–307 (2000), https://www.sciencedirect.com/science/article/pii/S000292970762254X.

21. *Who's Making Money from your DNA*?, BBC (Mar. 2, 2019), http://www.bbc.com/capital/story/20190301-how-screening-companies-are-monetising-your-dna.

22. *Supra* note 19, at 13771–78

therefore the use of their DNA is merely an effective means to an end in a crime solving scheme.

Genetic Privacy and the Third-Party Doctrine

***

Electronic surveillance law, as a controversial issue, first reached the United States Supreme Court sixty years before the advent of DNA forensics, when, in 1928, federal law enforcement wiretapped a bootlegger's home.[23] According to the Supreme Court in *Omstead*, law enforcement's actions posed no Fourth Amendment violation: "There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing, and that only. There was no entry of the houses or offices of the defendants."[24] However, Justice Brandeis, in a virulent dissent, reminded the Court that "Crime is contagious. If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means—to declare that the Government may commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution."[25]

Later, the Court changed its viewpoint in a series of cases that took place nearly ten years before the first use of DNA in criminal investigations, cases concerned with the legality of law enforcement surveillance mechanisms, including: *Katz v. United States*;[26] *United States v. Miller*;[27] and *Smith v. Maryland.*[28] These cases set Fourth Amendment limitations on government intrusions and solidified the concept of a reasonable expectation of privacy in an private individual's communications, except in those cases where data is transferred to third-parties.[29]

23. Olmstead v. United States, 277 U.S. 438 (1928).

24. *Id*. at 465.

25. *Id*. at 468.

26. Katz v. United States, 389 U.S. 347, 88 S. Ct. 507 (1967); *see also* Berger v. New York, 388 U.S. 41 (1967).

27. United States v. Miller, 425 U.S. 435, 96 S. Ct. 1619 (1976).

28. Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577 (1979).

29. Richard M. Thompson & Jared P. Cole, *Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA),* CONG. RESEARCH SERV., R44036 (May 19, 2015), https://www.epic.org/crs/R44036.pdf. It is important to note that there are communications, and there are other bits of information like meta data,

In *Katz*, decided in 1967, the Court noted that the Fourth Amendment protects people (not property) and that there is no need for a physical violation to be present for a privacy violation to have occurred. According to Justice Steven's majority opinion, once it is "recognized that the Fourth Amendment protects people—and not simply areas—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[30] After *Katz*, the government argued that the privacy rights discussed in the case, that are now enshrined in the Wiretap Act, are forfeit once information is turned over to a third-party. This concept is now referred to as the third-party doctrine.[31]

In 1976, in *Miller*, the Court examined the case of yet another bootlegger, this time running an unregistered operation without the intention to pay taxes on the some one-hundred and seventy-five gallons of whiskey. Via subpoena, the government, led by the Treasury Department's Alcohol, Tobacco and Firearms Bureau ("ATF"), sought to have bank records from all of Miller's activities divulged.[32] The appeals court held that the government had improperly circumvented the defendant's Fourth Amendment right against unreasonable searches and seizures by "first requiring a third party bank to copy all of its depositors' personal checks and then, with an improper invocation of legal process, calling upon the bank to allow inspection and reproduction of those copies."[33] However, the Supreme Court upended the lower court's holding and any expectation of privacy in data held by third-parties by noting that, "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the

certain location data, etc. The boundaries of what can and cannot be construed a communication is constantly shifting.

30. *Katz*, 389 U.S. 347.

31. The Wiretap Act, 18 U.S.C. § 2511 (1968) (The Wiretap Act, officially Title III of the Omnibus Crime Control and Safe Streets Act, attempted to codify the Fourth Amendment principles solidified in *Katz*. The Wiretap Act: 1). The Wiretap Act prohibits the unauthorized, nonconsensual interception of "wire, oral, or electronic communications" by government agencies as well as private parties; 2) establishes procedures for obtaining warrants to authorize wiretapping by government officials; and 3) regulates the disclosure and use of authorized intercepted communications by investigative and law enforcement officers.).

32. *Miller*, 425 U.S. at 435.

33. *Id*. at 439.

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."[34]

In Justice Brennan's dissent, he noted the underlying dilemma presented in the case, the concept that the "bank, a detached and disinterested entity, relinquished the records voluntarily. But that circumstance should not be crucial. For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[35] The inability of an individual to divorce him or herself from the general workings of the national economy was of incredible importance to Justice Brennan, who noted that, because a person doesn't have the option to disengage from the banking world, they inevitably reveal a great deal of their personal information to third-parties, and thereby the government. The majority's belief that an individual "assumes the risk" and consents to violations of his or her privacy by simply engaging in the public sphere, especially through something as necessary as banking, would allow only those individuals who are completely divorced from society to hold a reasonable expectation of privacy in their information.[36] Justice Brennan noted that individuals who entrust their funds to a bank are revealing their, "personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography."[37]

The majority chose not to contemplate the collateral consequences of their decision in *Miller*; however, Justice Brennan's intuitive dissent foreshadowed the future concerns of privacy jurisprudence regarding the third-party doctrine. He wrote that the Court's decision, "while concerned in the present case only with bank statements," "opens the door to a vast and unlimited range of very real abuses of police power."[38] Justice Brennan's intuition about the inability to divorce oneself from banking, echoes theories about the interconnectedness of one's DNA. Hacker and geneticist

34. *Id*. at 441.

35. *Id*. at 451.

36. *See* Peter Goldberger, *Consent, Expectations of Privacy, and the Meaning of Searches in the Fourth Amendment*, 75 J. CRIM. & CRIMINOLOGY 319 (1984), https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=6424&context=jclc.

37. *Miller*, 425 U.S. at 435.

38. *Id*. at 451.

Yaniv Erlich has concluded that over 90% of Americans can be found on the basis of familial DNA alone, and researchers at Baylor University have noted the propensity of genetic-testing sites to turn individuals into unwilling, and unknowing, "criminal informants vis-à-vis their own families."[39]

In *Smith*, the Court further eroded the holding of *Katz* as applied to the privacy of information held by third-parties.[40] The Court found that the petitioner did not have a legitimate expectation of privacy regarding the numbers he dialed because those numbers were automatically turned over to a third-party, in this case, the phone company. The Court also ruled that even if the petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation was not one that society deemed reasonable. Thus, the Court concluded that installation of the pen register was not a search where a warrant would be required.[41] By echoing the holding in *Miller*, the *Smith* Court further expanded the third-party doctrine.

In their dissent to *Smith*, Justice Stewart and Justice Brennan held a staunch defense of privacy, and of their interpretation of *Katz*.[42] The Justices noted that, "[i]t is simply not enough to say, after *Katz*, that there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them to the police."[43] When examining the reasonable expectation of privacy of a phone user, the two Justices declared their doubt anyone would want revealed "the most intimate details of a person's life."[44] The virulent *Miller* dissent, joining the dissent in *Smith*, embraces a strict privacy doctrine and looks to the holding of *Katz* to provide guidance for how to approach privacy cases arising out of new technologies and new means of governmental intrusion.

The Supreme Court, in both *Miller* and *Smith,* overreached the holding of *Katz,* diverging from precedent and allowing for massive invasions of privacy in the name of the third-party doctrine. These cases set forth the framework for cases involving genetic

39. Guerrini et al., *supra* note 10, at 1.

40. Katz v. United States, 389 U.S. 347, 88 S. Ct. 507 (1967).

41. *See Justice Information Sharing: Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act),* U.S. DEPT. OF JUST., https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284 (last updated Sept. 19, 2013).

42. Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577 (1979).

43. *Id.*

44. *Id*. at 749.

material, at a time when the technology allowed for a more limited matching scheme than it does today. In 2013, in *Maryland v. King*, the Court, in a 5-4 decision, ruled that "taking and analyzing a cheek swab of the arrestee's DNA is… a legitimate police booking procedure that is reasonable under the Fourth Amendment."[45] The *King* holding, however, limited the taking and retention of genetic material to individuals convicted of crimes and noted that the "expectations of privacy of an individual taken into police custody necessarily are of a diminished scope" when compared with the rights enjoyed by everyday citizens. The Maryland Court noted that a DNA swab could be taken following an "arrest supported by probable cause to hold for a serious offense."[46] The Court emphasized that a "sample may not be added to a database before an individual is arraigned."[47]

It is important to note that the *King* holding did not state that DNA testing is *not* a Fourth Amendment search. Rather, the Court found that buccal swabbing is a search under the Fourth Amendment, but that the need for a warrant was diminished given that the arrestee was already in police custody for a serious offense and his or her arrest was precipitated by probable cause. The Court notes the importance of DNA to potentially exonerate arrestees, as well as a way to identify "who has been arrested and who is being tried."[48]

Because of this, the Court inquired into whether the search was reasonable, versus whether the search lacked individualized suspicion. Finding that, the Court addressed the individualized suspicion prong. The Court turned to reasonableness and found that

45. See Maryland v. King, 569 U.S. 435, 133 S. Ct. 1958 (2013); See also Brief for Elec. Privacy Info. Ctr. et al., as Amici Curiae Supporting Respondents, Maryland v. King, (2013) (No. 12-207), https://epic.org/amicus/dna-act/maryland/EPIC-Amicus-Brief.pdf. In an amicus brief, numerous privacy experts warned that because "there is no statutory requirement for the government to discard the full DNA sample from which the DNA profile is obtained, the government indefinitely remains in possession of a person's full genetic makeup." *Id.* at 2. Furthermore, "As science reveals new ways in which DNA may be used, the potential for misuse by government entities presents a risk to individual privacy. Already, state governments have authorized law enforcement DNA samples to be used for non-law enforcement purposes." *Id.*

46. *Maryland v. King*, 569 U.S. 435, 464 (2013).

47. *Id*.

48. *Id*.

an arrestee would have a lessened expectation of privacy when compared to a member of the general public.

Furthermore, the *King* Court noted that, in terms of the processing of DNA, the detainee's DNA "loci came from noncoding DNA parts that do not reveal an arrestee's genetic traits and are unlikely to reveal any private medical information."[49] In contrast, individuals who have sent in a buccal swab to genetic-testing services reveal substantial information about their medical and genealogical traits. In fact, due to evolving technology since *King* was decided in 2013, services like Ancestry.com and 23andMe are marketed to test consumer genomes for certain diseases. At last count, the Food and Drug Administration had approved 23andMe to test for ten genetic sequences associated with risk factors for disease, including diseases such as Parkinson's, Alzheimer's and Celiac's.[50]

The uploading of an unidentified suspect's DNA to a commercial website is qualitatively different than the taking of a buccal swab from an arrestee. First of all, an arrestee has to be identified and formally accused of a serious crime prior to being subject to a swab. Furthermore, while arrestees are limited in their ability to argue that they have a reasonable expectation of privacy, members of the general population are not. Because arrestees have this notice, they are less likely to be caught unawares regarding the search. Furthermore, arrestees whose DNA has been collected may have that DNA uploaded to the CODIS system, whereby they can expect certain privacy and safety procedures to be undertaken. For example, information as to their health and genetic predispositions are left out of a CODIS analysis, whereby such information is a feature of commercial websites. Although a lowered expectation of privacy is to be expected when engaged in the punitive process, the rules for incarcerated individuals should not apply across the board, nor should government intrusions be celebrated in the interests of catching offenders at the expense of genetic privacy.

The Supreme Court in *Riley v. California,* could be seen as eroding the strong statements made in *King* regarding the negligible

49. *Id*.

50. Press Release, U.S. Food & Drug Admin., *FDA allows marketing of first direct-to-consumer tests that provide genetic risk information for certain conditions* (Apr. 6, 2017), available at https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm551185.htm.

nature of a police intrusion.[51] As a narrow holding, *King* still applies to identifying arrestees, but attempts to expand the holding and apply the framework to crime solving involving the DNA of non-arrestees fail on multiple grounds.[52] The *King* Court was divided 5-4 on the issue of DNA testing arrestees, with Justice Scalia writing a virulent dissent on behalf of himself and Justices Ginsburg, Sotomayor, and Kagan. The majority applied a general standard of reasonableness, weighted against legitimate government interests. The *King* Court put forward two very different views of DNA. The first was that, "the only difference between DNA analysis and the accepted use of fingerprint databases is the unparalleled accuracy DNA provides."[53] The second was that, "the intrusion of a cheek swab to obtain a DNA sample is a minimal one."[54] These varying perspectives, one looking to the database search and one looking to the physical search that taking a DNA sample entails, showcases the complexity of the issue. The Court did note that revealing more genetic characteristics about prisoners, other than their identity, would pose "additional privacy concerns not present here."[55] *Riley* is applicable as to these additional privacy concerns. *Riley* asked whether the government could inspect digitally stored information pursuant to a search incident to arrest. The *Riley* Court echoed the *King* Court, by stating that cell phones, like DNA, have "immense storage capacity."[56] The *Riley* Court, considering the privacy concerns of law enforcement being able to access digitally stored data, held—unanimously—that government agents must obtain a warrant to conduct such a search. The *Riley* Court attempted to distinguish itself from *King*, by stating that the vast quantity and numerous different types of personal information revealed by searching the digital contents of a cell phone were dramatically different from the one kind of information, mere identity, that is revealed by the DNA sample.[57] This analysis is, of course, becoming

51. Riley v. California, 134 S. Ct. 2473, 2494–95 (2014).

52. *See generally* Jennie Silk, *Calling Out Maryland v. King: DNA, Cell Phones, and the Fourth Amendment*, 51 CRIM. L. BULL 1212 (2015), available at https://ssrn.com/abstract=2553606).

53. *Id*. at 1971.

54. *Id*. at 1972.

55. *Id*. at 1979.

56. *Riley*, 134 S. Ct. at 2489.

57. *See* Andrew Pincus, *Evolving Technology and the Fourth Amendment: The Implications of Riley v. California,* CATO SUPREME COURT REVIEW (2014),

ever more complicated as more and more information can be revealed about a person through DNA testing as the technology evolves.

This tension between legitimate government interests and privacy rights continues to be tested. When *Carpenter* was accepted by the Supreme Court, many experts were intrigued by the incredible possibilities the case posed for data privacy.[58] Orin Kerr noted that the acceptance of *Carpenter* was a "momentous decision" and that it was not an "exaggeration to say that the future of surveillance law hinges on how the Supreme Court rules in the case."[59] Privacy proponents were intrigued with whether the third-party doctrine, if collapsed by the *Carpenter* Court, would force law enforcement to either obtain a warrant for CSLI data they once found easy to retrieve via subpoena under *Miller* and *Smith*. [60]

The *Carpenter* Court noted that the case raised two important issues. The first was whether a person has a expectation of privacy in his physical location and movements and the second is whether a person has a reasonable expectation of privacy in information voluntarily turned over to third parties. The answer to both questions was yes. While law enforcement had previously been relying on court orders[61] and subpoenas, the standard of suspicion for those was considerably lower than the probable cause requirement of a warrant. In a fairly narrow holding, the Court

https://object.cato.org/sites/cato.org/files/serials/files/supreme-court-review/2014/9/pincus.pdf.

58. Carpenter v. United States, 138 S. Ct. 2206 (2018); *see also* Orin Kerr, *Supreme Court Agrees to Hear 'C*arpenter v. United States*,' the Fourth Amendment Historical Cell-Site Case*, WASH. POST (June 5, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/05/supreme-court-agrees-to-hear-carpenter-v-united-states-the-fourth-amendment-historical-cell-site-case/?utm_term=.a9a104f0b7b4.

59. *Id*.; *see also* Brief for Orin Kerr as Amici Curiae Supporting Respondent, Carpenter v. United States, 138 S. Ct. 2206 (2013) (No. 16-402), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3047300.

60. *Id*.

61. These orders are often referred to as 2703(d) orders, under 18 U.S.C. § 2703. There is an argument to be made that genetic information is a communication protected against 2803(d) orders under ECPA. Although this paper does not delve into that topic too deeply, such a finding would allow for greater protections. The DOJ has not issued its own determination. *See Justice Information Sharing*, U.S. DEPT. OF JUST., https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last updated Apr. 23, 2019).

eroded the third-party doctrine set forth by *Miller* and *Smith*, opting to return to a more *Katz*-esque world whereby people, and not property, are the intended beneficiaries of privacy protections.

If the *Carpenter* Court held that there is a reasonable expectation of privacy in one's location, it is reasonable too for individuals to hold a similar, if not stronger expectation, in the privacy of their genetic information. In a PLOS survey of Amazon Mechanical Turks, researchers for the Medical Ethics and Health Policy recently found that respondents are 10% more likely to agree to the statement that law enforcement should be able to search cell phone records for investigative purposes following a violent crime, than they are to agree that law enforcement should be able to require DTC companies to require information about their customers.[62] Furthermore, while CSLI requires multiple inquiries in order to continuously track individual's movements, DNA only needs to be uploaded once to be viable for law enforcement purposes forever. The sequence-once-inquire-forever nature of DNA means that law enforcement will have the means to continue running searches ad infinitum.

The nature of DNA sequencing prompts a different analysis that one typically undertaken in order to garner a warrant. Typically, law enforcement need a warrant in order to get into something, generally something of a physical or tangible nature. For example, law enforcement may need warrants to de-encrypt cell phones or open the trunks of cars. In the case of genetic information however, law enforcement may have already sequenced a genome, and may be utilizing a genealogy website to upload the information they already have, in hopes of garnering a hit, or a match. Rather than attempting to break a physical barrier, law enforcement is attempting to interject information into a closed system in the hopes of tracing that information. Warrants to access information in such a system is less like the warrants mentioned above, and are more akin to the Network Investigative Technique ("NIT") warrants. NIT warrants allow law enforcement to create and deploy malware that augments content from websites to instruct user computers to send identifying information to the government. Such warrants were used

62. Guerrini et al., *supra* note 10, at 1. The researchers warned that "far from being a forensic anomaly, the public genetic search that led to the arrest of the Golden State Killer suspect is quickly on its way to becoming routine procedure. *Id.*

in a recent string of child pornography cases, the "Playpen" cases.[63] While such warrants are arguably incredibly invasive, numerous circuits have held that there was a good faith exception that allowed for their execution. Like NIT warrants, a warrant to search a genealogy database requires the use of that site's infrastructure, and law enforcement is generally not looking for any certain individual with particularity. For example, in the NIT cases, it was any user of the site, any individual who downloaded pornographic materials. In genealogy sites, the search would be tailored to any user with certain genetic markers. These types of warrants deviate from the typical warrant scope, but as technology outpaces the law, new and diverse forms of warrants are bound to develop.

Justice Gorsuch, in his *Carpenter* dissent, noted that, if the court were to allow *Smith*, *Miller* and *Katz*, to govern in the DTC genetic-testing context, it would yield a ridiculous result. He stated, "[c]an [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."[64] Gorsuch recommended scrapping the third-party doctrine, and instead adopting an approach centered on property law. He believes that the voluntariness of turning over personal information to a third-party who may or may not reveal that information to law enforcement is suspect, and that "knowing about a risk doesn't mean you assume responsibility for it."[65] Gorsuch states that, "[w]henever you walk down the sidewalk you know a car may negligently or recklessly veer off and hit you, but that hardly means you accept the consequences and absolve the driver of any damage he may do to you."[66]

Countering the concept of consent, Gorsuch writes, "I confess I still don't see it. Consenting to give a third party access to private papers that remain my property is not the same thing as consenting to a search of those papers by the government."[67] While Gorsuch's property-centric approach is sensical when applied to those users signing up for genetic-testing websites, and sending in their DNA, it becomes distorted when applied in the context of

63. *See* United States v. Ganzer, 922 F.3d 579 (5th Cir. 2019). Nine circuits have ruled against suppression of NIT warrant related information.

64. Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018).

65. *Id*. at 2263.

66. *Id*.

67. *Id.*

familial matching. In the context of familial matching, an individual need not even be aware that one of their relatives has effectively furnished law enforcement with their genetic-information. The car that hits the pedestrian, in Gorsuch's example, may as well have been a UFO plowing into someone's home—striking someone who not only didn't consent to walking in the street, but didn't even know implicit dangers of alien conveyances. Most consumers of genetic-testing companies are unaware that the service they pay for can be used as a de facto law enforcement database, and there is no reason for Americans who haven't voluntarily had their DNA sequenced to be aware of the dangers to their privacy posed by the practice.

Although privacy proponents may agree on the application of *Carpenter* to DNA housed by what might be termed "proprietary websites"[68] like 23andMe and Ancestry.com, there is some disagreement over the privacy of DNA once it is voluntarily turned over to a secondary website. Some proprietary websites allow consumers the option of downloading their own data, which can then be uploaded to another website like GedMatch, in order to find more relatives or learn more about genetic conditions. This, some experts argue, is akin to posting your DNA data on a public channel, lowering the reasonable expectation someone might have in the privacy of their genetic-information. However, those sites do cater only to genealogists and hobbyists, and users would be hard pressed to ascertain that law enforcement does use the site.

Therefore, while Americans do hold a significant expectation of privacy in their DNA, even if they voluntarily turn it over for commercial purposes, there is a an even more intimate violation in regards to familially matching someone's DNA who has not consented to even a commercial search. While legally, both sets of individuals deserve similar protections, it seems grossly unfair to run familial searches against individuals who have simply had the ill-luck of being genetically related to someone who has subscribed to a consumer genetic-testing service. Given the holding in *Carpenter*, it appears the government would have a difficult time asserting that DNA information being held by a third-party genetic-testing website, regardless of whether the information was voluntarily given or not, is undeserving of Fourth Amendment protections. However, recent lower court decisions have refused to extend Carpenter to invasive searches. Therefore, while jurisprudentially, it wouldn't be much of an extension to apply

68. Credit given to Albert Gidari, Consulting Director of Privacy at the Stanford Center for Internet and Society.

Carpenter to genetic information, most lower courts have been loathe to extend *Carpenter* at all.

Several recent cases have showcased how unwilling district courts are to extend *Carpenter* to anything besides historical geolocation tracking. According to one district court, tower dump searches can be "sufficiently definite" when supported by a warrant based on probable cause. That court also determined that even if the search warrants lacked probable cause or were insufficiently particular, a good faith-exception would preclude suppression.[69] Another district court decided that eBay purchase records are not protected under *Carpenter.* That court declined to extend the *Carpenter* holding to defendant's online commercial transactions. In reaching its conclusion, the court relied on the voluntariness of defendant's commercial transaction, finding that defendant had "exposed" his information, therefore assuming the risk that eBay would reveal his personal information to law enforcement.[70] *Carpenter* is being applied quite narrowly, at least in the short period of time since the opinion was penned, to cases scrutinizing tower dumps,[71] IP addresses,[72] and Internet of Things (IOT) data searches.[73] If challenged today, an individual's claim that law

69. *See* United States v. James*,* No. 18-cr-216, 2018 WL 6566000 (D. Minn. Nov. 26, 2018).

70. *See* United States v. Schaefer, No. 3:17-cr-00400-HZ, 2019 WL 267711 (D. Or. Jan. 17, 2019).

71. *See* United States v. James, No. 18-cr-216, 2018 WL 6566000 (D. Minn. Nov. 26, 2018) (holding that tower dump searches are "sufficiently definite" when supported by a warrant based on probable cause)*; see also* United States v. Adkinson, 916 F.3d 605 (7th Cir. 2019) (holding that *Carpenter* did not invalidate warrantless tower dumps, nor did it address searches by private parties).

72. *See* United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018) (stating that an IP address "falls comfortably within the scope of the third-party doctrine."); *see also* United States v. Monroe*,* 350 F.Supp.3d 43 (D. R.I. 2018) (finding that an argument based on a reasonable expectation of privacy in an IP address is "untenable"); United States v. Felton*,* 367 F. Supp. 3d 569 (W.D. La. 2019) (reasoning that that postal service logs showing when a defendant tracked a USPS package do not fall under *Carpenter*.); United States v. Gregory, No. 8:18-CR-139, 2018 WL 6427871 (D. Neb. Dec. 7, 2018) (finding that subscriber information that merely "incidentally" reveals location information is not covered by *Carpenter*).

73. *See* Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521 (7th Cir. 2018) (holding that a collection of smart meter data at fifteen minute intervals is a Fourth Amendment search); *see also* United States v. Kay, No. 17-CR-16, 2018 WL 3995902 (E.D. Wis. Aug. 21, 2018) (rejecting a

enforcement violated his or her reasonable expectation under *Carpenter* by collecting his or her DNA from a genealogy company would be a difficult one to make. Therefore, it might be necessary to carve out a new area of the law to cover genetic data, an area that relies on the reasonable expectation of privacy concept but extends that concept to genetic material.

However, rather than rely on case law, or at least as a placeholder until such case law is established, it might be easier to frame potential future arguments as policy-based. Therefore, the best mechanism for stopping potential abuse is to craft legislation, privacy policies, and best practices designed to encourage companies to not infringe on their consumer's rights. Relying on case law should yield a positive decision in cases like these, especially from the point of view of a privacy proponent, but that type of reactive solution is an uphill battle. Finding positive preventative solutions could help stop problems before they occur.

DNA and Abandonment

***

The issue of abandonment is perhaps the most logical argument in favor of allowing law enforcement to sequence DNA left at a crime scene. Because the Fourth Amendment applies to physical boundaries, like protecting an individual's home, car, or even geolocation, the Fourth Amendment generally fails to protect DNA information. According to Professor Elizabeth Joh, who worked as a law clerk during the *United States v. Kincade* case, "[w]e leave traces—skin, saliva, hair, and blood—of our genetic identity nearly everywhere we go."[74]

In the *Kincade* decision, which remarked on accruing and retaining the DNA of parolees, Judge Kozinski, in his dissent, remarked that, "[w]e can't go anywhere without leaving a

Carpenter-based challenge to a pole camera); In re Search of, 317 F. Supp. 3d 523 (D. D.C. 2018) (finding that compelled biometric searches can fall within the scope of a warrant); United States v. Kubasiak, No. 18-CR-120, 2018 WL 6164346 (E.D. Wis. Aug. 23, 2018) (finding that a video camera pointed at defendant's backyard does not violate *Carpenter's* holding); Demo v. Kirksey, No. 8:18-cv-00716-PX, 2018 WL 5994995 (D. Md. Nov. 15, 2018) (finding that six months of data accrued by a GPS unit in a diaper bag can violate a reasonable expectation of privacy).

74. *See United States v. Kincade,* 345 F.3d 1095 (9th Cir. 2003)*; See also* Elizabeth Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U. L. REV. 857, 858 (2006); *see also* United States v. Kincade, 345 F.3d 1095 (9th Cir. 2003).

breadcrumb trail of identifying DNA matter. If we have no legitimate expectation of privacy in such bodily material, what possible impediment can there be to having the government collect what we leave behind, extract its DNA signature and enhance CODIS to include everyone?"[75] However, while the principle of abandonment has served as a basis for gathering DNA samples, it has never been lawfully extended to the testing of said DNA. While law enforcement can gather DNA on tissues, and cups, and cigarettes from anyone, inputting the DNA into a database should constitute a separate search which must be met with a probable cause requirement.[76] Uploading abandoned DNA to CODIS it met with requirements from the site as well.

The Supreme Court in *Carpenter* recognized the idea that certain third-party data information gathered via pen register is distinguishable from something as invasive as cell-site location information.[77] Likewise, DNA is an example of other third-party-held information that is, arguably, "qualitatively different" and therefore deserving of utmost protections under the Fourth Amendment.[78] An individual's genetic material houses information as to an individual's sex, hair color, height, weight, biological relatives, risk factors for certain medical conditions, and more. Furthermore, DNA serves as a basis for a near perfect match to DNA held on file at anytime in the future. Unlike cell-site location information, DNA provides data that is constant and unyielding. While an individual can vary his or her movements, no one can alter their molecular self. Protections that cite the invasive nature of CSLI need to be extended to genetic information, at risk of law enforcement obtaining the most perfect means of biometric surveillance yet.

HIPAA and GINA

***

75. *Kincade,* 345 F.3d at 1045.

76. *See generally* Joh, *supra* note 74; *see also* David Kaye, *Science Fiction and Shed DNA,* SSRN (Dec. 8, 2006), https://ssrn.com/abstract=950572.

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

78. Matt Ford, *How the Supreme Court Could Rewrite the Rules for DNA Searches,* THE NEW REPUBLIC (Apr. 30, 2018), https://newrepublic.com/article/148170/supreme-court-rewrite-rules-dna-searches (presenting an argument before the *Carpenter* decision was issued about how the case could shine light on the issue of abandoned DNA).

Genetic privacy, as a healthcare field, has been relatively well-understood for some years. Both the Health Insurance Portability and Accountability Act (HIPAA) and the Genetic Information Nondiscrimination Act (GINA) offer protections for consumers when it comes to the disclosure of their DNA. However, neither offer protections against intrusions by law enforcement.

In order to fall under HIPAA safeguards, genetic data must fulfill two general requirements. First, the data must be personally identifiable, and second, it must be maintained by a HIPAA covered healthcare provider, health plan, or healthcare clearinghouse. As to the first point, genetic material does fall into the personally identifiable or PII realm. With an individual's DNA, law enforcement can, with a high degree of certitude, pinpoint his or her identity. It is the second aspect that disallows HIPAA from governing information accrued by consumer DTC genetic-testing websites. Such websites do not fall under the respective umbrellas of healthcare provider, health plan, or healthcare clearinghouse. Because such genetic-testers market directly to consumers, and don't fall under a general definition of healthcare, the privacy measures that would protect genetic-material given to a doctor or other provider do not extend to the DNA consumers send to corporations.

Under GINA, genetic data is protected from attempted intrusions on the part of employers and health insurance providers. However, GINA offers no protections against law enforcement requests for genetic data. Until the passage of a federal privacy law that protects DNA as a biometric that cannot be accessed without a warrant, there needs to be mechanisms in place to ensure that genetic-testing websites do not run afoul of the Fourth Amendment. Furthermore, if, or perhaps when given the recent rise in proposed bills, federal privacy legislation is passed in the United States, DNA needs to be classified as a biometric deserving of Fourth Amendment protections.

The Future of Genetic Privacy

***

There are numerous social gains to be made through the adoption and use of evolving DNA technologies. The apprehension of sexual and violent predators is just one of the many benefits that such technology has furnished. However, these net gains must be careful balanced against the propensity of the technology to come with risks. Consumer privacy cannot be easily regained once it is lost. An individual's DNA profile can be sequenced once, and then

retained forever. That profile can identify individuals reaching back, laterally, and even forward across a family tree.

Without understanding the true benefits of genetic testing, it is hard to develop a full picture of what rights Americans should give up in order to garner certain benefits. The Center for Disease Control's (CDC) Thousand Genome project aims to add "new types of biological information over time, including transcriptomic, proteomic, metabolomics, and epigenetic information."[79] That project in particular is expected to yield valuable scientific insights on the molecular underpinnings of health and disease states. The project offers scientific macro benefits, as well as potential micro consumer benefits. The project notes that those benefits include a sense of certainty or control that comes along with having knowledge about potential health risks, diseases, or predispositions. There is the benefit of exploring a family tree or meeting long lost relatives.

With the evolution of DNA technologies, legal protections need to be adopted quickly in order to protect genetic privacy. The benefits of genetic testing need not be hampered by the imposition of regulatory controls. Third party websites should not be in the business of data collection, nor should law enforcement be able to utilize consumer sites without some form of governmental oversight. Rapid DNA testing is becoming less costly, and as the cost and time barrier lessens, law enforcement will begin to see DNA testing as an easy crime solving route. Crime solving is far less intrusive than other potential uses (or misuses) of genetic data.[80]

DNA "magic boxes," rapid DNA testing machines that generate results in as little as ninety minutes, have recently found homes in police booking stations.[81] Such technologies push the

79. W. Gregory Feero et al., *From One Hundred Thousand Genomes in the United Kingdom to Millions of Genomes in the United States: What Lessons Can we Learn?*, CDC: GENOMICS AND PRECISION HEALTH (Dec. 1, 2016), https://blogs.cdc.gov/genomics/2016/12/01/from-one-hundred/.

80. Tonya Riley, *Using 23andMe to Reunite Families at the Border Comes With Serious Privacy Risks*, MOTHER JONES (June 22, 2018), https://www.motherjones.com/politics/2018/06/using-23andme-to-reunite-families-at-the-border-comes-with-serious-privacy-risks/.

81. *See* Heather Murphy, *Coming Soon to a Police Station Near You: The DNA 'Magic Box,'* THE NEW YORK TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/science/dna-crime-gene-technology.html (looking into Magic Boxes); *see also* Lauren Kirchner, *DNA Dragnet: In Some Cities, Police Go From Stop-and-Frisk to Stop-and-Spit*, (Sept. 12, 2018),

boundaries of privacy, and demand swift responses. These machines are now being fitted with the capability to automatically upload results to CODIS for matching purposes. Furthermore, bigger consumer companies are entering the crime solving space.[82] States need to ensure that they have updated familial matching legislation in place, and that their approach towards genealogical websites keeps in mind the privacy rights of everyday Americans.

Privacy Policies

***

Many popular DTC companies leave the decision over whether the company will reveal your DNA information to law enforcement in the company's hands. There are no enforcement mechanisms to ensure that the companies voluntarily enter into privacy agreements with consumers, nor are there many oversight mechanisms in place to ensure that those promises are followed once made. The best way to categorize DTC genetic-testing companies is to place them as more or less privacy conscious on a spectrum, by examining the four main aspects of their privacy policies.

The first aspect is transparency, and whether the company elects to reveal to the public how many law enforcement requests have been made regarding data. Transparency reports are important in holding companies responsible for their interactions with law enforcement. The second aspect is in regards to notice, and whether the company elects to provide adequate notice to individuals whose user information has been inquired after. The third aspect is whether the DTC allows access to PII pursuant only to a warrant, or whether the company maintains autonomy over they fulfill informal requests or comply with subpoenas. Finally, the fourth aspect is whether the site maintains the expectation that consumers are sending in their own DNA, and no one else's, to be sequenced. DTC companies can do this by asking consumers to physically or e-sign agreements that the DNA they are testing

https://www.propublica.org/article/dna-dragnet-in-some-cities-police-go-from-stop-and-frisk-to-stop-and-spit (looking into DNA dragnetting).

82. Peter Aldhous, *The Golden State Killer Case Has Spawned A New Forensic Science Industry*, BUZZFEED NEWS (Feb. 15, 2019, 12:43 PM), https://www.buzzfeednews.com/article/peteraldhous/genetic-genealogy-dna-business-parabon-bode.

belongs to them.

Company	Risk Level	Notice Provided	Court Order Required	Transparency Reports	User Agreements	Crypto-Signature	Warrant Required
23andMe	Low-to-Moderate	Yes	Yes	Yes	No	No	No
Ancestry.com	Moderate	Yes	Yes	Yes	No	No	No
FamilyTreeDNA	Moderate	Yes	Yes	No	No	No	No
Veritas Genetics	High	No	No	No	No	No	No
MyHeritage	High	No	No	No	No	No	No

In the interests of gauging consumer understanding, and the adequacy of various privacy policies utilized by popular DTC companies, I have included the above infographic. The genealogy websites listed all have privacy policies that range from low-to-moderate risk to high risk for consumers who are concerned with the privacy of their genetic material. Although this list is by no means exhaustive, and may not be reflective of the companies' actual practices, it may serve as a good indicator of the types of promises DTC companies engage in with their consumers.

Such policies, although not protective against law enforcement probes, often detail how much information they will impart to law enforcement officers upon request. It is worth noting that, after the above graphic was completed, the Associated Press revealed that FamilyTreeDNA has been giving unprecedented access to its genealogical information to the FBI. Therefore, the language each company uses in their respective privacy policies matters very little in relation to the actual practices they carry out. It is important to look beyond the scope of privacy policies, and concentrate on the actual practices of companies to see whether they are fulfilling their privacy and security promises they have made to their consumers.

Following the news of the FamilyTreeDNA breach, the Future of Privacy forum dropped the company from its list of

companies engaging in best practices.[83] Those best practices required a legal process for the disclosure of genetic data to law enforcement and transparency reporting on at least an annual basis.[84] According to those best practices, "Genetic Data may be disclosed to law enforcement entities without Consumer consent when required by valid legal process. When possible, companies will attempt to notify Consumers on the occurrence of personal information releases to law enforcement requests."[85]

The president of FamilyTreeDNA apologized to the site's users for failing to disclose that it was sharing DNA data with federal investigators working to solve violent crimes.[86] FamilyTreeDNA's president, Mr. Greenspan, did not apologize for the practice itself, but merely how it was communicated: "I am genuinely sorry for not having handled our communications with you as we should have… We've received an incredible amount of support from those of you who believe this is an opportunity for honest, law-abiding citizens to help catch bad guys and bring closure to devastated families."[87] However, public shaming is not enough to ensure that companies are acting on the promises they have made to their consumers.

The language of each DTC company differs when it comes to whether they give PII to law enforcement:

1. 23andMe states that they "use all practical legal and administrative resources to resist [law enforcement]

83. *See* Cat Zakrzewski, *Consumer Advocates Want Washington to Tackle 'Wild West' of DNA Test Kits*, DAILY HERALD (Mar. 2, 2019, 6:00AM), https://www.dailyherald.com/business/20190302/consumer-advocates-want-washington-to-tackle-wild-west-of-dna-test-kits (explaining how FPF dropped FamilyTreeDNA as a signatory onto its best practices); *see also Privacy Best Practices for Consumer Genetic Testing Services*, FUTURE OF PRIVACY F. 16 (July 31, 2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf, (last accessed Apr. 25, 2019).
84. *Id*.
85. *Id*. at 10.
86. Matthew Haag*, FamilyTreeDNA Admits to Sharing Genetic Data With F.B.I.,* NEW YORK TIMES (Feb. 4, 2019), https://www.nytimes.com/2019/02/04/business/family-tree-dna-fbi.html (omitting, as usual, a definition as to what would constitute a violent crime).
87. *Id*.

requests." Their transparency report is updated on a quarterly basis.[88]

2. Ancestry's privacy statement states the company will disclose PII only to "Comply with valid legal process (e.g., subpoenas, warrants)." Furthermore, the site follows a notice process and issues an annual transparency report, detailing how many law enforcement requests the company receives and what information is disclosed.[89]
3. FamilyTreeDNA's privacy policy states that the site only shares DNA to "comply with a valid legal process (e.g., subpoenas, warrants)." The site promises that "[i]f compelled to disclose your Personal Information to law enforcement, we will do our best, unless prohibited by law, to provide you with notice." The site does not issue a transparency report.[90]
4. Veritas Genetics' privacy policy outlines that they will give out PII if "we believe necessary or appropriate in connection with an investigation of illegal activity."[91]
5. MyHeritage promises to take "appropriate steps to ensure that transfers of personal information are done in accordance with applicable law and carefully managed to protect your privacy rights and interests." The company does not issue a transparency report.[92]

Although it is arguable that the mere existence of disclaimers within a privacy policy serves as the basis for meaningful and informed consent, it would appear that if a consumer were to read the language quoted above, he or she would be under the assumption that the DTC would fight to keep his or her genetic information private. Using all legal routes available to resist law enforcement attempts at garnering information, paints the picture of a consumer

88. *Transparency Report,* 23ANDME.COM, https://www.23andme.com/transparency-report/ (last visited May 20, 2019).
89. *Ancestry Guide for Law Enforcement*, ANCESTRY.COM, https://www.ancestry.com/cs/legal/lawenforcement (last visited May 20, 2019).
90. *FamilyTreeDNA Privacy Statement,* FAMILYTREEDNA.COM, https://www.familytreedna.com/legal/privacy-statement (last updated May 07, 2019).
91. *Privacy & Legal*, VERITASGENETICS.COM, https://www.veritasgenetics.com/privacy-legal (last visited May 20, 2019).
92. *MyHeritage Privacy Policy,* MYHERITAGE.COM, https://www.myheritage.com/privacy-policy (last updated Oct. 07, 2019) May 20, 2019).

and a DTC working in conjunction against the government. Does the language referenced in privacy policies serve to reinforce or erode a consumer's reasonable expectation of privacy?

A reasonable consumer reading such privacy policies may note the remote possibility of a law enforcement officer being privy to his or her genetic details, but a remote possibility does not defeat a user's reasonable expectation of privacy. A reasonable consumer would assume that his or her DNA is being processed for the very reasons it was furnished, to match him or her with distant relatives, provide insights into genealogical ancestry, and perhaps point out a propensity for certain genetic diseases. The reasonable assumption here is that the consumer is not furnishing his or her DNA as a means for police intrusion and surveillance, and that revealing that his or her DNA has been or could be used for such purposes would be fairly shocking. Knowledge of the possibility of being surveilled is not enough to imply consent, nor is it enough to defeat the notion of a reasonable belief in the privacy of one's DNA.

In the case of an unsuspecting fourth party like DeAngelo, if we assumed law enforcement utilized a site like Ancestry or 23andMe, not only does the language of the privacy policies describe instances of law enforcement deceptively using a DTC website and claiming they had rights over the DNA, but those policies indicate that the websites will do everything in their power to protect consumer data. If the DTC website receives a court order or subpoena, they would have the ability to refuse to comply, or at the very least provide notice to the consumer. In DeAngelo's case, due to familial matching, he would never have been expected to read or implicitly agree to the site's privacy policy.

Because public-facing promises on genetic testing websites may not give a full picture of actual company policy regarding dealing with law enforcement, interviews with privacy counsel may shed more light on the issue. Therefore, in the interests of transparency, the following attorneys agreed to interviews whereby they ranked their perception of their site's privacy protections, and extrapolated on any additional safeguards their sites provide.

Recommendations for Law Enforcement

***

Rather than move forward with the current model whereby police intrusions are expected, pending a court decision to the contrary, law enforcement should be proactive about protecting citizen privacy. Agencies, both federal and state, can issue policy guidelines to federal or local law enforcement with

recommendations for how officials should engage with DTC companies. Approaching this issue from an informed and multi-faceted standpoint will allow solutions in administrative and legal policies that will help guide and also constrain law enforcement in their crime solving efforts. In the interests of crime solving, one does not necessarily need to sacrifice certain privacy interests, including the reasonable expectation of privacy one holds in their own DNA.

Agencies like state attorneys general offices, mayoral offices, and gubernatorial offices have a vested interest in ensuring their citizen's privacy. While crime solving is incredibly admirable, it does not need to come at the expense of privacy violations.[93] Law enforcement have incredible leeway in their ability to question witnesses, utilize CODIS on unidentified suspect's DNA, and even take a suspect's DNA upon arrest. Requiring law enforcement to obtain a warrant based on probable cause prior to engaging in a search of DTC companies is not too much to ask. State agencies, and even law enforcement heads, should take it upon themselves to advise law enforcement officers of the proper protocol for obtaining a warrant rather than searching a DCT website in the absence of probable cause.

While the Department of Justice has issued an interim policy regarding the use of genetic DTCs, that policy does not do enough to protect individual's civil liberties.[94] At the moment, that policy does two positive things. First, limits the problematic practice of allowing federally funded law enforcement from pretending to be a consumer while, in actuality, sending in crime scene DNA. Second, it prohibits law enforcement from profiling individuals on the basis of certain genetic markers. However, the policy fails to elucidate the Department's policies on warrants and it also fails to limit the practice of familial matching.

A more suitable advisory memo can be modeled after the one below.

93. Russell Brandom, *Police are using DNA Testing to Track Down a Fetus's Mother,* THE VERGE (May 10, 2018, 3:03 PM), https://www.theverge.com/2018/5/10/17340666/dna-testing-georgia-fetus-codis-abortion-genetics-investigation (outlining the DNA testing of fetal remains found in wastewater as an example of a privacy violation that might arise in the municipal context).

94. Katelyn Ringrose, DOJ Doesn't Go Far Enough to Limit Searches of Consumer Genetic Services, THE HILL (OCT. 4, 2019, 11:00AM), https://thehill.com/opinion/technology/463835-doj-doesnt-go-far-enough-to-limit-searches-of-consumer-dna-services.

Model Advisory Memo for Law Enforcement

***

The purpose of this memorandum is to explain the function of genealogical websites as relates to law enforcement. Genealogy websites such as Anscestry.com and 23andMe.com exist to connect consumers with family members, and help such consumers learn about potential health hazards, as well as learn about their genealogical history.

The popularity of the Golden State Killer case has popularized the notion of utilizing genealogical DNA databases for crime solving purposes. However, there are guidelines that law enforcement must follow in order to ensure citizen privacy.

Our state follows the guidelines instituted by CODIS. We are writing to remind law enforcement that we are as dedicated to crime solving as we are to protecting our citizens' privacy rights. Genealogical websites are not as reliable as results accrued by CODIS. Given the privacy concerns associated with using public genealogical websites, as well as the efficacy of such sites over the scientific benefits offered by a law enforcement database, we encourage law enforcement to turn to CODIS for their needs.

If the use of a genealogical website becomes necessary, then a warrant must be granted before such a website can be utilized. Moving forward, utilize law enforcement databases for DNA searches. If a search of such a website is absolutely necessary, you must receive a warrant in order to utilize information from a genealogical website. The information must be narrowly tailored, specific and only used as an identifier of the individuals who have submitted their DNA.

Recommendations for DTC Genetic-Testing Companies

***

DTC companies also have a part to play in ensuring that their privacy policies are designed to protect consumers against law enforcement intrusions. Rather than have varying levels of risk built into their business models, companies should hold their consumer's data private against law enforcement intrusions. The issue of DNA marketing to third-parties, including data brokers who sell information to law enforcement, should be addressed in both company policies and legislation.

Model Privacy Policy Regarding Requests from Law Enforcement

***

(a) THE COMPANY will not sell, lease, give, or rent your individual-level personally identifying information to any third party.
(b) THE COMPANY will not accept DNA uploaded to our database without the explicit consent of the individual whose DNA has been obtained, unless it can be proven that the individual is deceased.
(c) THE COMPANY requires authentication that customers are submitting their own DNA, or DNA belonging to a deceased individual, through a two-factor authentication system.
(d) THE COMPANY will not share Personally Identifying Information (genetic or otherwise) with any public databases.
(e) THE COMPANY will not provide Personally Identifying Information (genetic or otherwise) to an insurance company or employer.
(f) THE COMPANY will not provide information to law enforcement or regulatory authorities unless required by law to comply with a valid search warrant for genetic or personal information.
(g) THE COMPANY will provide you with notice prior to a valid search warrant, unless barred by court order.
(h) THE COMPANY will destroy Personally Identifying Information (genetic or otherwise) upon the consumer's request.
(i) THE COMPANY will destroy any Personally Identifying Information (genetic or otherwise) pursuant to a user failing to sign into their COMPANY account within a five (5) year period.
(j) For more information on THE COMPANY's policies regarding law enforcement, see our annual transparency report.

Legislative Oversight

***

Rather than begin with legislative oversight, this paper has purposefully covered tactics that would allow law enforcement and DTC companies the ability to act as market forces when it comes to the data sharing and brokerage of genetic materials. These two bodies are the ones engaging in the practice of the genetic privacy violations and are arguably the best situated to stop consumer

privacy harms before, or even if, the situation rises to a level warranting legislation.

There is a concept in cybercrime, codified by the CFAA,[95] whereby an offender can be said to have breached a computer by exceeding his or her authorized access. This means that computer users, perhaps when utilizing computers owned by the entity they work for, have intentionally obtained data that trespassed the line delineating the scope of their employment and the information that is illegally obtained. This concept can be utilized when it comes to a search of genealogical databases. Law enforcement may run a search of a direct match on a genealogical DTC site, but they will exceed their authorized access, bypassing the scope of their warrant, if they attempt to run familial matches. This is unlikely to be a physical barrier, for example workers do not need to hack the computers they are using to access illegal content or content that is privy to their organization. Rather, the theoretical framework differentiates data sets into those that are acceptable for access, and those data sets that aren't. Similarly, law enforcement will not have a physical barrier disallowing them from running a familial search, but will have a theoretical barrier differentiating direct matches from familial matches. If law enforcement exceeds the scope of their warrant by running a familial match, they should be held to criminal standards.

Given recent changes in the United States, as well as abroad, privacy law is becoming more of a popular topic. However, most privacy legislation is centered around commercial activities, like the regulation of personal data sold between companies for advertising purposes. Less attention is being paid to the surveillance mechanisms employed by law enforcement. Privacy legislation regarding DNA may be slow to adopt, as the technology adoption and evolution eclipses the law. Despite companies and law enforcement agencies being arguably better equipped to quickly enact meaningful change, it is important for legislative efforts to set the bar for such efforts. Therefore, legislation, at the very least, should address the following two areas of concern. The first is that any DNA database search, with the exception of CODIS, requires a warrant for probable cause on the basis of a sexually motivated and/or violent offense. The second is that individuals cannot run any familial matches on a DNA or genealogical database, except as necessary to participate in CODIS.

95. *See* 18 U.S.C. § 1030.

Legislation on this topic is very new, and as of yet fairly fledgling. Maryland, in its 2019 legislative session introduced House Bill 30, which bans anyone "from performing a search of any DNA or genealogical databases for the purpose of identification of an offender in connection with a crime for which the offender may be a biological relative of the individual from whom the DNA sample was acquired."[96] Maryland has also categorically banned familial searches on CODIS, and the existing loophole allow for officers to search public databases and not governmental databases remains open pending the passage of HB 30. The Maryland bill imposes criminal sanctions on individuals found in violation of the law, with up to five years imprisonment and/or a $5,000 fine.[97] In addition to this punitive measure, the bill also prohibits anyone from willfully keeping a DNA sample after receiving notification that the sample should be destroyed. Violators who willfully keep DNA on file after notification of a destruction order can be punished with up to one year in prison or a maximum fine of $1,000.[98]

The model legislation below is based off of Maryland's proposal, and directly addresses the issue of law enforcement utilizing genealogical databases. However, states might find it easier to integrate amendments into already existing biometric laws. If states do not want to completely foreclose the option of searching a genealogical database, but would instead like to leave the option of a warrant requirement open, that can be included as an option.

Model State Legislation Barring DNA Database Searches

***

Search of DNA Database

FOR the purpose of prohibiting a person from performing a search of a DNA or genealogical database for the purpose of identification of an offender in connection with a crime for which the offender may have his or her DNA in a database or be a biological relative of the individual from whom the DNA sample was acquired.

(a) Each DNA record of identification characteristics that results from DNA testing shall be stored and maintained

96. H.B. 30, 2019 Leg., Reg. Sess. (Md. 2019), available at https://legiscan.com/MD/bill/HB30/2019.
97. *Id*.
98. *Id*.

by the Crime Laboratory in the statewide DNA database system only, except as necessary to participate in CODIS.
(b) Each DNA sample shall be stored securely and maintained by the Crime Laboratory only in the statewide DNA repository.
(c) Typing results shall be stored securely in the statewide DNA database System only.
(d) A person may not perform a search of the statewide DNA database or any other DNA or genealogical database for the purpose of identification of an offender in connection with a crime for which the offender may have his or her DNA in a database or may be a biological relative of the individual from whom the DNA sample was acquired.

Model State Legislation Requiring a Warrant for DNA Database Searches

***

FOR the purpose of requiring probable cause prior to the performance of a search of a DNA or genealogical database for the purpose of identification of an offender in connection with a crime for which the offender may have his or her DNA in such a database or be a biological relative of the individual from whom the DNA sample was acquired.

(a) Absent a warrant for probable cause on the basis of a sexually motivated and/or violent offense, each DNA record of identification characteristics that results from DNA testing shall be input into and maintained by the Crime Laboratory in the statewide DNA database system only, except as necessary to participate in CODIS.
(b) Database searches made pursuant to a warrant must be made in a manner to limit the search to that of direct matches, identification matches to violent and/or sexually motivated offenders, and not familial matches, or matches made indicating a biological relative of the individual from whom the DNA sample was acquired.
(c) A person may not run a familial search on a DNA or genealogical database, except as necessary to participate in CODIS.

Conclusion

***

Warrantless searches of consumer DNA databases are unlawful exercises of police power. Intrusive searches, like those undertaken on such websites, must be based on a warrant requiring probable cause. There are multiple ways to combat the issue of law enforcement utilizing DTC websites in order to ascertain direct or familial matches. Such solutions include better company privacy practices, law enforcement buy in as related to privacy interests, and legislation that strictly regulates law enforcement's ability to engage in such searches. A holistic approach is necessary as the technology related to familial DNA matching becomes more pervasive. I hope this note functions as the basis for robust discussion on the future of genetic privacy. Through a multi-faceted approach that addresses private, law enforcement, and legislative solutions, violations of genetic privacy can be addressed and combated.