California Western Law Review

Volume 55 | Number 2 Article 8

7-29-2019

From Swabs to Handcuffs: How Commercial DNA Services Can Expose You to Criminal Charges Rebecca Gold

Rebecca Gold

FROM SWABS TO HANDCUFFS: HOW COMMERCIAL DNA SERVICES CAN EXPOSE YOU TO CRIMINAL CHARGES

TABLE OF CONTENTS

INTRODUCTION

Have you ever wondered if you are related to a famous historical figure? With a genealogy analysis costing less than a night out on the town, millions of people have swabbed their cheeks out of curiosity to discover more about their heritage. Ranging in price from $69 to $200, commercial DNA businesses analyze DNA samples and provide users with detailed information about themselves and their family. Cool, right? Think again. Suddenly, these customers have willingly exposed their most private information—their living selves—to the entire world. Without even realizing it, these customers have reduced their expectation of privacy. The Fourth Amendment generally prohibits

unreasonable searches and seizures.[1] However, information a person shares with third parties *can* be freely accessed by the police.[2] Under the "third-party doctrine," police can obtain information from a third party without a warrant, even though the person has not directly disclosed the information to the police.[3] Thus, if you willingly share information with others, you are willingly relinquishing your right to privacy.[4]

Modern technology inevitably clashes with outdated precedent, creating the need to reevaluate the scope of the third-party doctrine. This includes the type of information that the doctrine exempts from Fourth Amendment protections. Does it matter with whom the information is being shared? Do changes in modern social customs require a new analysis of the third-party doctrine when it comes to DNA? Primarily, police obtain DNA data from the Combined DNA Index System ("CODIS"), a police database consisting of DNA collected from lawful arrests and other stages of law enforcement.[5] However, as consumer websites like Ancestry.com continue to accumulate mass amounts of DNA, police should be entitled to use these databases as investigative aids. Police investigations can benefit from using commercial DNA services to connect familial, or even direct, DNA matches to solve crimes, but at what cost? Thus, the critical legal and societal question is how to strike the appropriate balance. New judicial rulings, which reduce the third-party doctrine's scope, open the door for the development of procedures to secure sensitive information.

As digital communication expands, expectations of privacy regarding all types of information are at odds with the archaic application of both the third-party doctrine and the original concept of the expectation of privacy. Applying these doctrines in the modern era requires a new understanding of privacy. Preserving the intent of the

1. U.S. CONST. amend. IV.
2. *See infra* Part I Section A.
3. *See generally* United States v. Miller, 425 U.S. 435 (1976).
4. *Id.*
5. *See* Natalie Ram, *Fortuity and Forensic Familial Identification*, 63 STAN. L. REV. 751, 760–61 (2011) ("Pursuant to . . . legislation, the FBI pioneered the Combined DNA Index System (CODIS)—a central database into which participating states and agencies can 'load' the genetic profiles they lawfully acquire and search among the profiles made available by other jurisdictions").

doctrines in the current decade will protect the people and ensure that the government can access only what is warranted under modern standards. This requires weighing the benefit of warrantless access to DNA against the loss privacy rights. In our world of ubiquitous and increasingly impersonal digital communications, it is time to re-evaluate the pivotal role of the expectation of privacy.

This Comment will address how the third-party doctrine conflicts with DNA privacy in light of the popularity of commercial DNA websites geared to the public. Part I explains the premise of the third-party doctrine and provides examples where police incriminate suspects based on DNA from websites, evidencing the investigatory latitude the third-party doctrine provides to accessing publicly collected DNA. Part II discusses how online privacy trends and the Supreme Court's *Carpenter* decision foreshadow the limits of the third-party doctrine. Part III explains how a limited third-party doctrine could prevent exploitation of privacy on DNA websites where users voluntarily relinquish their most sensitive personal data. Part IV proposes solutions to privacy issues resulting from police access to commercial DNA databases under the third-party doctrine.

I. THE THIRD-PARTY DOCTRINE APPLIED TO COMMERCIAL DNA

Online DNA testing companies offer a wide array of services and are both vast in number and consumer popularity. There are dozens of DNA testing companies across the Internet, and over twelve million people have used one or more DNA companies to test their genetic code.[6] DNA testing has become so popular that there is now even a market for pet DNA kits.[7] The most well-known DNA testing companies are Ancestry.com and 23andMe.com, but other popular companies include MyHeritage.com, FamilyTreeDNA.com, and LivingDNA.com.[8] As of 2017, there are 39 direct-to-consumer genetic

6. Antonio Regalado, *2017 Was the Year Consumer DNA Blew Up*, MIT TECH. REV. (Feb. 12, 2018), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up/.

7. *See* Eric Griffith, *The Best Dog DNA Testing Kits for 2019*, PC (Dec. 17, 2018), https://www.pcmag.com/roundup/364005/the-best-dog-dna-testing-kits.

8. *See* Mark Orwig, *Best DNA Test for Ancestry*, SMARTER HOBBY, https://www.smarterhobby.com/genealogy/best-dna-test/ (last updated Mar. 2019).

testing companies worldwide.[9] These companies offer a variety of services, depending on the company's method of testing and the services purchased. For instance, Ancestry.com offers users information about their relatives and family tree, whereas 23andMe.com provides health-related information based on a person's genetic makeup.[10] Some websites are built on an open-sharing platform, which allows users to directly compare their data with other users, while other websites act in a closed universe setting and do not share user data.[11]

However, DNA databases pose civil and criminal privacy concerns because DNA companies and government agencies may have access to the user's information. This raises the concern of tracking where the information goes after a user participates in a DNA testing service. As expected, the user has access to their DNA results, but unbeknownst to most customers, consumer DNA companies often retain the contractual rights to use the DNA results or information however they choose.[12] These rights include giving user-provided DNA to medical studies and selling the information to other third parties.[13] As consumer protection lawyer Joel Winston said, "[i]t's basically like you have no privacy, they're taking it all."[14] For example, companies like Ancestry.com can continue using the DNA even after the user's death.[15]

9. Sheldon Krimsky & David Cay Johnston, COUNCIL FOR RESPONSIBLE GENETICS, ANCESTRY DNA TESTING & PRIVACY: A CONSUMER Guide 2 (2017), http://www.councilforresponsiblegenetics.org/img/Ancestry-DNA-Testing-and-Privacy-Guide.pdf.

10. *See* Orwig, *supra* note 8.

11. *Id*. (describing certain DNA websites allow users to contact matches, while other websites are more restrictive).

12. *See* Kristen Brown, *What DNA Testing Companies' Terrifying Privacy Policies Actually Mean*, GIZMODO (Nov. 18, 2017, 10:10 AM), https://gizmodo.com/what-dna-testing-companies-terrifying-privacy-policies-1819158337 (discussing how DNA testing websites have ownership rights to genetic information users send them).

13. *Id*.

14. *Id*.

15. *Id*. ("Even though Ancestry says they don't really own your DNA . . . they [do] own rights to it. They could test it in 100 years from their freezer for whatever purpose they want").

Further, sharing DNA with these businesses may diminish users' right against warrantless searches and self-incrimination.[16] The third-party doctrine determines whether law enforcement can access this information and what legal steps are required to access the data.[17] Since the third-party doctrine permits warrantless searches of *any* information given to third parties, and DNA websites are third parties, the third-party doctrine could technically give police complete access to consumer DNA databases.[18] In fact, recent criminal cases shed light on how the third-party doctrine presently and routinely enables police to utilize consumer DNA databases, despite concerns about privacy and law enforcement accuracy.[19]

A. How the Third-Party Doctrine Was Born

The third-party doctrine is an exception to the Fourth Amendment's general prohibition against warrantless searches and seizures, and has developed from a number of Supreme Court cases.[20] Under this exception, any information a person relays to a third party is not protected against warrantless searches.[21] The third-party doctrine, which was established in the 1970s by *Smith v. Maryland* and *United States v. Miller*, applies to *any* information someone voluntarily discloses to a third party.[22] Both of these cases rely on the "expectation

16. *See* Glen Martin, *Gird Your Genes: What DNA Matching Might Mean for Your Privacy*, CAL. MAG. (July 24, 2018), https://alumni.berkeley.edu/california-magazine/just-in/2018-07-24/gird-your-genes-what-dna-matching-might-mean-your-privacy (explaining individuals who voluntary give their DNA to open-source DNA platforms are effectively waiving their reasonable expectation to privacy).

17. *Id*.

18. *See id*. ("Uploading information to GEDmatch and similar sites involves implicit consent: by using the site, you agree to surrender your information to the public domain.").

19. *Id*.

20. *See, e.g*., Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

21. *See generally Smith*, 442 U.S. at 743–44 (holding there is no expectation of privacy to phone numbers dialed on a phone where the phone numbers were automatically disclosed to a third party upon placing a call); *Miller*, 425 U.S. at 449–50 (holding defendant did not have an expectation of privacy to bank records voluntarily made available to the public).

22. *See generally Smith*, 442 U.S. at 744; *Miller*, 425 U.S. at 443.

of privacy" standard from *Katz v. United States* to determine whether the information gathered without a warrant constitutes an illegal search.[23] In *Katz*, the violation of one's "expectation of privacy" became the standard to determine whether a search occurred, eliminating the former physical trespass requirement.[24]

In *Miller*, the government accessed a suspect's bank records without a warrant.[25] There was no expectation of privacy for the bank records because they were not confidential communications.[26] Rather, the defendant voluntarily revealed the information to the bank, a third party.[27] The Court held that police can access such information "even if the information is revealed on the assumption that it will be used only for a limited purpose."[28] Following *Miller*, the Court's holding in *Smith* expanded the third-party doctrine to encompass phones.[29] This case reinforced that voluntary conveyances of information to a third party, here a phone company, erodes an individual's expectation of privacy.[30] Even though the defendant believed this was private information, the Court concluded that the defendant "assumed the risk" the phone company could reveal the information to others, including the police.[31] As a result, the warrantless access to the information was permitted.[32]

In an attempt to find balance between privacy in the digital age and police investigation tactics, the Court has analyzed reasonable expectations of privacy in a variety of different technologies. A notable application of the expectation of privacy occurred in *United States v.*

23. *Smith*, 442 U.S. at 742–44 (1979); *Miller*, 425 U.S. at 442.

24. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (holding "the 'trespass' doctrine . . . can no longer be regarded as controlling" when evaluating whether a search has taken place).

25. *Miller*, 425 U.S. at 436.

26. *Id*. at 442 ("[C]hecks are not confidential communications but negotiable instruments to be used in commercial transactions").

27. *Id*. (finding a person should not expect privacy when handing information to a third-party).

28. *Id*. at 443.

29. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

30. *Id*. at 744.

31. *Id*. (concluding defendant "voluntarily conveyed numerical information to the telephone company and . . . [i]n so doing . . . assumed the risk that the company would reveal to police the numbers he dialed").

32. *Id*. at 745–46.

Jones, which is the first of a handful of cases to define appropriate means of information gathering in light of technological advancements. In *Jones*, the police followed the defendant's car for over twenty-eight days using a GPS tracker that police surreptitiously installed onto the car.[33] This long period of surveillance abused the basic principle that police could follow a person on public roads.[34] In a split opinion, the Court decided that the extensive tracking constituted an impermissible warrantless search, but the divided court did not agree on a unified rationale.[35]

Maintaining privacy has become a societal concern as the prevalence of social media increases. The third-party doctrine, which was first developed in the 1970s, "turned heavily on the limited forms of interaction in a prior technological era."[36] However, as social media use has increased, a tweet about what you had for breakfast can be instantly viewed by thousands of people you may or may not directly know. Social media, text messaging, online shopping, and other services allow the average American to share a significant amount of information with others daily.[37] Through the current application of the third-party doctrine, police and other governmental agencies can easily access this information without legal constraint. As one article notes, "Communications, commerce, and finance increasingly take place online and operate through private intermediaries; accordingly, the third party doctrine has left an immense amount of personal information unprotected by the Fourth Amendment."[38] The lack of legal safeguards for accessing personal information online, extends to previously inaccessible genetic information. Although the availability of personal data, including genetic information, can improve police investigations, there are concerns about over-extending government control and eroding the Fourth Amendment.[39]

33. United States v. Jones, 565 U.S. 400, 403 (2012).

34. *Id*. at 412.

35. *Id*. at 411–13.

36. Lucas Isaacharoff & Kyle Wirschba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 987, 987–88 (2016).

37. *See id*. (discussing the limits of the third-party doctrine in the digital age).

38. *Id*. at 988.

39. *Id*.

B. The Third-Party Doctrine and DNA: Recent Cases Solved by DNA

Historically, most public concern with the dissemination of DNA website data involved its use in civil claims, specifically insurance disclosures and employment discrimination.[40] However, commercial DNA databases have recently been used in criminal cases. Under the third-party doctrine, police can use DNA websites in criminal investigations without needing to get a warrant.[41] Commercial DNA websites and other companies that analyze DNA are enhancing investigations and narrowing down suspect lists. The ability to compare DNA samples from website users, which were intended for fun and entertainment, could potentially lead to police turning commercial databases into a secondary CODIS system. Two recent cases that have used commercial DNA to identify suspects are the Golden State Killer case and the April Tinsley murderer. Each case remained unsolved until new DNA advancements narrowed down the suspect list. These cases reveal how new DNA technology has the potential to not only solve current crimes, but to go back in time and bring closure to cold cases.

1. The Golden State Killer Controversy

The Golden State Killer is a well-known California murder case, which had gone unsolved for over forty years, until DNA websites came into the picture.[42] The Golden State Killer murdered twelve people, raped forty-five others, and committed over 100 home burglaries over a ten-year span.[43] The killer was never caught, and the case turned cold. A break in the case finally arrived when someone uploaded their DNA

40. Eric Rosenbaum, *5 Biggest Risks of Sharing Your DNA With Consumer Genetic-testing Companies*, CNBC (June 16, 2018, 10:00 AM), https://www.cnbc.com/amp/2018/06/16/5-biggest-risks-of-sharing-dna-with-consumer-genetic-testing-companies.html?__twitter_impression=true.

41. Bradley Henry, *Third-Party Doctrine: What Is It and Why Does it Matter?*, HENRY L. (June 21, 2016), www.henrylawny.com/third-party-doctrine-matter/.

42. *See* Bruce Brown, *DNA Link to Golden State Killer Raises Questions of Privacy Versus Safety*, FOX NEWS (Apr. 30, 2018), http://www.foxnews.com/tech/2018/04/30/dna-link-to-golden-state-killer-raises-questions-privacy-versus-safety.html.

43. *Id*.

to GEDMatch.com.[44] GEDMatch.com is an "open source," platform, and the users are warned by the company that their information may be "accessed for uses other than ancestry searches."[45] Using the DNA database from this website, police found a positive familial match from a consumer's DNA sample and DNA found at one of the crime scenes from the Golden State Killer.[46] This DNA match allowed police to track Joseph DeAngelo, the alleged Golden State Killer.[47] DeAngelo is now on trial for the crimes perpetrated by the Golden State Killer.[48] The success of the Golden State Killer case has sparked a movement to find other killers, such as the Doodler and the infamous Zodiac Killer, using consumer DNA databases.[49]

2. April Tinsley and DNA Facial Sketches

Just a few weeks after the news broke about the commercial DNA used to identify the alleged Golden State Killer, police used DNA services to track down April Tinsley's murderer.[50] April Tinsley was an eight-year-old girl from Indiana who was abducted, raped, and killed in 1988.[51] Tinsley's killer was never caught despite leaving an abundance of DNA behind.[52] More disturbingly, Tinsley's murderer

44. *Id*.

45. *Id*.

46. *Id*.

47. *Id*.

48. Sam Gross, *Alleged Golden State Killer Makes Second Appearance in Court; Set to Return May 29*, RENO GAZETTE J. (May 14, 2018, 1:10 PM), https://www.rgj.com/story/news/crime/2018/05/14/golden-state-killers-trial-delayed-until-may-29/608581002/; *see also* Amelia McDonell-Parry, *What's Next for Alleged Golden State Killer*, ROLLING STONE (Aug. 24, 2018, 2:16 PM), https://www.rollingstone.com/culture/culture-news/golden-state-killer-joseph-deangelo-whats-next-715368/ (noting the case is ongoing and does not have a final ruling yet).

49. *See, e.g.*, Nick Watt, *This Serial Murder Case Has Been Cold for More Than 40 Years. Now Police Say They Have a Suspect*, CNN (June 21, 2018, 5:32 PM), https://www.cnn.com/2018/06/20/us/doodler-cold-case-murders/index.html (discussing the importance of DNA in solving crimes such as the Doodler murders).

50. Eric Levenson & Amanda Watts, *Child-Killer Taunted Investigators for 30 Years With Disturbing Notes. DNA Ends the Mystery of Who Did it, Police Say*, CNN (July 17, 2018, 6:52 PM), https://www.cnn.com/2018/07/16/us/cold-case-april-tinsley-dna-trnd/index.html.

51. *Id*.

52. *Id*.

left sickening notes threatening to kill more young girls in the area.[53] Even though the police had the suspect's DNA, they could not match it with the databases available at the time.[54]

After news outlets detailed the arrest of the Golden State Killer, the investigators of Tinsley's case decided to give DNA identification another shot and sent their crime scene sample to Parabon Nanolabs.[55] Parabon Nanolabs uses DNA samples from other commercial DNA companies like Ancestry.com and GEDmatch.com to make a possible facial image of the unknown match.[56] Unlike the Golden State Killer case, which primarily relied on matching the murderer's DNA with a relative, Parabon Nanolabs used the crime scene samples from Tinsley's murder to create a possible sketch of her killer.[57] This facial information narrowed the suspect pool to two people – the Miller brothers, John and JPM. Police collected DNA samples from John Miller's trash, which positively matched the 1988 sample.[58] A month later, John Miller confessed to killing Ashley Tinsley.[59] Using the Parabon Nanolabs facial creation software, police were able to successfully arrest John Miller, the dangerous man who threatened to strike again in 1990 and 2004.[60]

3. What These Cases Mean for Future DNA Use

Commercial DNA services, like Ancestry.com, aid law enforcement in two ways. First, these websites can provide a direct match or familial match that law enforcement can use to catch criminals, like the Golden State Killer. Second, other companies, such

53. *Id*.

54. *Id*.

55. *Id*.

56. Kate Snow & Jon Schuppe, '*This is Just the Beginning': Using DNA and Genealogy to Crack Years-old Cases*, NBC NEWS (July 18, 2018, 1:30 AM), https://www.nbcnews.com/news/us-news/just-beginning-using-dna-genealogy-crack-years-old-cold-cases-n892126.

57. *Id*.

58. Gina Martinez, *DNA Match Leads to Arrest in 1988 Rape and Murder of Indiana Girl After Decades of Taunts from Killer*, TIME (July 16, 2018), http://time.com/5339649/april-tinsley-indiana-murder-john-d-miller/.

59. *Id*.

60. *Id*.

as Parabon Nanolabs ("Parabon") and Identitias, can use these programs and databases to create sketches of suspects.[61] Founded in 2008, Parabon is a genetics company that recently expanded its application to criminal investigations.[62] Parabon offers a service called Snapshot.[63] Snapshot is a phenotyping program that uses known DNA samples to generate a composite facial image based on similarities between the unknown sample and Parabon's DNA database.[64] These facial images can be used by law enforcement to aid criminal investigations.

With the ease and availability of obtaining user DNA data, consumer DNA websites have the alarming potential to broaden the CODIS database to a greater scope than just the actual users. Commercial DNA websites can add exponentially more information because they can extrapolate information not just about the person who used the website but also the person's relatives. The ability to connect individuals through their DNA is the purpose of services such as Ancestry.com, which are specifically designed to connect people to their family.[65] As a result, each *individual* DNA sample as well as each *familial related match* is added to the police's search range, drastically increasing the data pool size. When cross referenced with commercial DNA data, one DNA sample can point police to a whole family tree, as shown by the Golden State Killer case. The police can not only gain physical access to twelve million individual DNA samples, but they also get the second cousin twice removed through a familial related match.[66]

Beyond direct familial connections, DNA technology reaches greater heights through genetic phenotyping. The individual, the

61. *See Parabon Snapshot Advanced DNA Analysis*, SNAPSHOT DNA ANALYSIS, https://snapshot.parabon-nanolabs.com/ (last visited May 1, 2019).

62. *About Parabon Nanolabs*, PARABON NANOLABS, https://www.parabon-nanolabs.com/nanolabs/about (last visited May 1, 2019).

63. Kate Snow, *Putting a Face to DNA: How New Tech Gives Hope in Cold Cases*, NBC NEWS (June 30, 2015, 4:47 PM), https://www.nbcnews.com/news/us-news/dna-mugshot-how-new-tech-gives-hope-cold-cases-n384771.

64. *Id*.

65. *See* ANCESTRY, https://www.ancestry.com/cs/ancestry-family (last visited May 1, 2019) (noting to users of the site the "more you grow your family tree, the more hints you'll get [to related family members]—a loop of discoveries").

66. Regalado, *supra* note 6.

second cousin, and any unknown matches with similar coding can be deduced. Phenotyping is a relatively new method of DNA identification but it is rapidly growing and being used in police investigations.[67] Rather than relying on a direct match or familial match, this genetic technology can sketch the person based on other similar DNA already collected by these companies.[68] Such technology provides more potential samples to compare to police-obtained evidence and could double the amount of information police can access.

Currently, the CODIS system holds thirteen million samples.[69] CODIS data is commonly used in criminal investigations. Potentially, every time police collect evidence from a crime scene, they can use CODIS to see if there is a match. Similarly, with genetic phenotyping, every additional sample from DNA websites improves the algorithm that predicts facial features of unidentified suspects whose DNA is not already in CODIS. These databases are now as large as the CODIS database, but the standards used to collect and analyze this information are not government regulated.[70] Although the Department of Defense has funded Parabon phenotyping research, standardization is not currently required.[71] With the abundance of easily accessible

67. *See* Snow, *supra* note 63 (observing Parabon's ability to use DNA left at crime scenes to produce sketches of suspects).

68. *Id*. "[Parabon] created a reference database of genomic data and the outward physical traits typically associated with those genes. Now, with each new sample, a mathematical model helps predict which traits that person has, based on their genetic code." *Id*.

69. *CODIS – NDIS Statistics*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics (last visited May 1, 2019).

70. *See* Regalado, *supra* note 6 (noting consumer data collecting websites often function frequently with little oversight from regulators).

71. *See Parabon Awarded Government Contract to Develop Next-Generation Forensic DNA Platform*, PARABON NANOLABS (Nov. 16, 2016), https://www.parabon-nanolabs.com/nanolabs/news-events/2016/11/keystone-next-generation-dna-forensic-platform-award.html (discussing Parabon's contract with the Department of Defense, which will eventually include implementing "the latest forensic DNA analysis tools under a single, easy-to-use platform"). Parabon Nanolabs has another contract with the Department of Defense to help identify unidentified military remains from past wars. *Parabon Awarded U.S. Department of Defense (DoD) Contract to Aid Identification of Unknown Remains from Past Conflicts*, PARABON NANOLABS (Jan. 27, 2016), https://www.parabon-nanolabs.com/nanolabs/news-events/2016/01/snapshot-afdil-contract-award.html.

information, abuse of these consumer DNA databases is along the horizon, although not many cases have come to light.

So far, police have not asked Ancestry.com directly for DNA information,[72] but the question is, will Ancestry have to hand over that information when the police come knocking on their door? Presently, Ancestry.com's Privacy Statement requires a valid warrant to disclose DNA information.[73] While this is nice contractual protocol, it falls short because technically police do not need a warrant for information voluntarily given pursuant to the third-party doctrine. In theory, police could force these websites to hand information over. In the alternative, officers can upload a sample they collected at a crime scene, enter the information into a commercial DNA website, like Ancestry.com, and use the service like any other consumer.

Even if Ancestry.com and other commercial DNA websites do not share their DNA information with law enforcement, phenotyping businesses can offer police the same information, if not more. Parabon, for instance, gathers DNA samples from both Ancestry.com and GEDMatch.com to fuel its Snapshot program.[74] In turn, Snapshot is promoted to law enforcement as a new innovative tool to fight crime.[75] Through this service, Parabon utilizes private DNA information originally entrusted to sites like Ancestry.com. Parabon gathers information from "public genetic genealogy" sources,[76] raising concerns about how the third-party doctrine applies to this context. Although Parabon may technically rely on public genetic genealogy sources, consumers are not aware of this information exchange. What once started out as a simple consumer-to-company interaction, transforms into a multi-layered exchange of information. Thus, the

72. *Ancestry 2017 Transparency Report*, ANCESTRY, http://www.ancestry.com/cs/transparency (last visited May 1, 2019).

73. *Your Privacy*, ANCESTRY, https://www.ancestry.com/cs/legal/privacy statement (last visited May 1, 2019) (noting to users if Ancestry is forced to disclosure personal information, it will provide "advance notice, unless . . . prohibited under the law from doing so").

74. *Snapshot Genetic Genealogy*, PARABON NANOLABS, https://snapshot.parabon-nanolabs.com/genealogy (last visited May 1, 2019).

75. *See Parabon Snapshot Advanced DNA Analysis*, PARABON NANOLABS, https://snapshot.parabon-nanolabs.com/ (last visited May 1, 2019) (highlighting the genetic technology used by law enforcement to identify the Golden State Killer).

76. *Id*.

privacy rights within the Ancestry.com and GEDMatch.com contracts might not be enough to protect consumers from other companies working with law enforcement. Just because consumers give up their DNA voluntarily to commercial websites, police should not be permitted to access the information by virtue of the information being "public."

According to Dr. Thomas May, a professor at Washington State University, "[o]ur current regulatory approach to privacy in direct-to-consumer (DTC) genealogy testing has permitted the creation of a Wild West environment."[77] Dr. May believes this regulation-free "Wild West environment" enabled the government to acquire the DNA leading to the arrest of Golden State Killer, Joseph DeAngelo.[78] Although consumer DNA websites have standard privacy policies, anyone, including law enforcement, can get around these privacy policies simply by purchasing a DNA kit and uploading a sample into the database as a user. The officers pursuing the Golden State Killer did not even have to get a warrant to find DeAngelo.[79] Instead, the officers simply uploaded the sample they had from the crime scenes into a commercial database to see if there was a match.[80]

II. SETTING THE PATH FOR HEIGHTENED PRIVACY PROTECTIONS

A. The Modern Expectation of Privacy

Consumers are concerned about the actual amount of privacy in digital services they use. Many people are attempting to take control of their privacy by going through measures online to "remove or mask their digital footprints."[81] However, according to the Pew Research Center, out of the 86% of people taking preemptive measures to maintain privacy, over 61% feel they can do more to secure their

77. Thomas May, *Sociogenetic Risks – Ancestry DNA Testing, Third-Party Identity, and Protection of Privacy*, 2018 NEW ENGLAND MED. J. 410, 411 (2018).

78. *Id*.

79. Brown, *supra* note 42.

80. *Id*.

81. Lee Raine, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/ (finding around "86% of users have taken steps online to remove or mask their digital footprints").

information.[82] Further, one survey showed that people view certain types of "public" information, such as email contents, as more invasive than pat downs or vehicle searches.[83] Consumers are concerned about who controls their information, who can collect their information, and where the information can be shared.[84] States are responding to this mass cry for privacy.[85] Recent developments in state law suggest a shift away from the original interpretation of "expectation of privacy." For instance, California has passed numerous digital privacy laws to increase digital security over the past few years.[86] California legislation strengthens online privacy on an array of digital forums by regulating online tracking, social media, and other personal online information.[87]

In the social media sphere of privacy, Facebook has reacted to the heightened expectation of privacy by modifying its privacy settings.[88] These changes were a result of users choosing to opt out of Facebook's services all together because of their digital privacy concerns.[89] In

82. *Id*.

83. Isaacharoff & Wirschba, *supra* note 36, at 995 n.54; *see also* Lee, *supra* note 81 (stating that 74% of the study found it 'very important' to have control over who gets their information, and 65% found it "'very important' to . . . control what information is collected about them").

84. Isaacharoff & Wirschba, *supra* note 36, at 995.

85. *See* Hannah K. Speirs et al., *Notable New State Privacy and Data Security Laws—Part Two*, S&W CYBERSECURITY & DATA PRIVACY L. BLOG (Feb. 20, 2017), www.swlaw.com/blog/data-security/2017/02/20/notable-new-state-privacy-and-data-security-laws-part-two/ (detailing state-level privacy reforms affecting education, data privacy, and business law).

86. *See, e.g*., Education Foundation, *Recent Online Privacy Legislation in California*, CONSUMER FED. OF CAL., https://consumercal.org/about-cfc/cfc-education-foundation/recent-online-privacy-legislation-in-california/ (last updated Feb. 19, 2016) ("California expanded its existing Student Online Personal Information Protection Act and its limits on operators' uses of student information to apply to preschool and prekindergarten students").

87. *See generally id*. (detailing recent privacy legislation in California from 2013 to 2015).

88. *See* Yuki Noguchi, *Facebook Changing Privacy Controls as Criticism Escalates*, NPR (Mar. 28, 2018, 12:08 PM), https://www.npr.org/sections/thetwo-way/2018/03/28/597587830/criticism-prompts-facebook-to-change-privacy-controls (explaining Facebook implemented changes in its privacy setting "after coming under intense public and regulatory pressure for unauthorized disclosures of private information to a third-party firm").

89. *Id*.

response, Facebook is making it easier for customers to change their privacy preferences.[90] Facebook's goal is to help reduce targeted advertisements, which use personal data.[91] These changes show that the "reasonable expectation of privacy" – the legal boundary between what is searchable and what is not – is expanding. Now, consumers are demanding to keep more areas private, even within the generally public forum of social media.

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

The recent trend of vigilantly protecting privacy rights is reflected in the 2018 United States Supreme Court decision, *Carpenter v. United States*.[92] This case examined whether police can conduct warrantless searches and seizures of cell phone records.[93] The Court in *Carpenter* held that the third-party doctrine does not extend to sensitive location data recorded by cell phone towers.[94] Traditionally, police were allowed to access phone records because they were considered public.[95] However, the Court decided in a narrow 5-4 decision that police need a warrant to search cell phone location data for extended periods of time.[96] The Court found that gathering the cell phone data is a search and requires a warrant due to the invasive location information stored.[97]

90. *Id*.

91. *See id*. (noting Facebook's privacy policy changes enable users to block the dissemination of their personal information to third-party advertisers).

92. 138 S. Ct. 2206 (2018).

93. *Id*. at 2211.

94. *Id*. at 2217.

95. *Id*.

96. *See* Curt Levey, *Supreme Court Ruling in Cell Phone Case is a Victory for our Privacy Rights*, FOX NEWS (June 22, 2018), http://www.foxnews.com opinion/2018/06/22/supreme-court-ruling-in-cell-phone-case-is-victory-for-our-privacy-rights.html; *see also* Amy Howe, *Opinion Analysis: Court Holds that Police Will Generally Need a Warrant for Cellphone Location Information (Updated)*, SCOTUS BLOG (June 22, 2018, 6:01 PM), http://www.scotusblog.com/2018/06/opinion-analysis-court-holds-that-police-will-generally-need-a-warrant-for-cellphone-location-information/ (noting the extended period of time could mean any time greater than seven days).

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

The defendant, Timothy Carpenter, was convicted of robbing multiple Radio Shacks with three other people.[98] Instead of getting a warrant, the police applied for a court order under the Stored Communications Act ("STA").[99] The STA requires a lower standard than probable cause to compel a third-party to disclose information.[100] Using months of cellular-based location records (over 127 days), the police discovered the exact location of both Mr. Carpenter and his co-defendant.[101] The appellate court determined that since the defendant voluntarily gave his information to the cell phone provider, he had a lesser expectation of privacy and was not entitled to Fourth Amendment protection.[102] The Supreme Court disagreed. Instead, the Court acknowledged the issues that high-tech information gathering systems present in light of the third-party doctrine. Expectations of privacy have transformed due to the drastic technological advancements since *Miller* and *Smith* were decided. When "*Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes."[103] If communication devices that could fit in your pocket were hardly imaginable in 1979, sending DNA to a website to analyze your genetic code was unfathomable.[104] DNA did not debut in criminal investigations until 1986, more than a decade after *Miller*; therefore, the

98. *Id*. at 2212.

99. *Id.* The Stored Communications Act allows the "Government to compel disclosure of certain telecommunications records when it 'offers specific and articulable facts showing that there are reasonable grounds to believe' that the records sought 'are relevant and material to an ongoing criminal investigation.'" *Id*.

100. *See id*. at 2221 (concluding a showing of "reasonable grounds" that the information sought is relevant to the investigation "falls well show of the probable cause required for a warrant").

101. Jennifer Lynch, *Symposium: Will the Fourth Amendment Protect 21st-Century Data? The Court Confronts the Third-Party Doctrine*, SCOTUS BLOG (Aug. 2, 2017, 12:21 PM), http://www.scotusblog.com/2017/08/symposium-will-fourth-amendment-protect-21st-century-data-court-confronts-third-party-doctrine/.

102. *Id*.; *see also Carpenter*, 138 S. Ct. at 2213.

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

104. Scientists are just beginning to analyze DNA. Two years before the third-party doctrine was created, scientists were only in the developmental stage of implementing sequencing techniques – years away from analyzing DNA like today. The Human Genome Project began roughly 20 years after the third-party doctrine was already in effect and was not completed until years later. *See The History of DNA Timeline*, DNA WORLDWIDE, https://www.dna-worldwide.com/resource/160/history-dna-timeline (last visited May 1, 2019).

third-party doctrine could not have been intended to extend to such sensitive matters.[105]

Another key underpinning of the Court's conclusion in *Carpenter* is how the "expectation of privacy" is defined in *Katz*.[106] Back in 1967, the *Katz* Court defined the expectation of privacy as "one that society is prepared to recognize as reasonable."[107] This "expectation of privacy" is the backbone of the third-party doctrine, which is based upon the expectation of privacy that arises when information is voluntarily shared.[108] Now, according to *Carpenter*, "[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."[109] In the context of today's hand-held device society, the *Carpenter* court found it was reasonable for the defendants to expect their locations over long periods of time to be private.[110] The "fact that the information is held by a third party does not by itself overcome the user's claim to the Fourth Amendment protection."[111] The government argued the third-party doctrine applies to cellular tracking information,[112] but the Court rejected the government's argument as a "significant extension" of the third-party doctrine to a new era of information.[113] The expectation of privacy afforded to cellular data was reasonable, and the Court decided

105. *See* Lisa CalandroDennis & J. ReederKaren Cormier, *Evolution of DNA Evidence for Crime Solving – A Judicial and Legislative History*, FORENSIC MAG. (Jan. 1, 2016, 3:00 AM), https://www.forensicmag.com/article/2005/01/evolution-dna-evidence-crime-solving-judicial-and-legislative-history (discussing the first time genetic evidence was admitted into court was in 1986 from expert witness, and molecular biologist, Alec Jeffreys).

106. *See* Katz v. United States, 389 U.S. 347, 351 (1967) (holding the Fourth Amendment "protects people, not places" therefore, "[w]hat a person knowingly exposes to the public" is not protected).

107. Smith v. Maryland, 442 U.S. 735, 740 (1979).

108. *Id*.; *see also* United States v. Miller, 425 U.S. 435 (1976).

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

110. *Id*. at 2218.

111. *Id.* at 2217.

112. *Id.* at 2218.

113. *Id*. at 2219.

there was no reduced expectation permitting police to access this data without a warrant.[114]

For now, the complete scope and application of *Carpenter* remains unknown. The Court asserted that its holding only applies to the collection of location-based data from cell towers.[115] The Court also opinioned its holding does "not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras."[116] However, the line between "conventional" techniques and techniques like location-surveillance is muddled. As technology advances and more invasive surveillance techniques become "conventional," *Carpenter*'s narrow scope will be tested. Future technology may qualify as "location-based," even though it may not directly provide location information. Paul Ohm, a law professor and information privacy expert, predicts that *Carpenter* will be extended to other investigatory tools. Ohm explains, "[t]he true test of the substantive sweep of *Carpenter* will be whether courts apply its reasoning to government access to databases full of sensitive and intimate information" that does not necessarily involve location information.[117] Focusing on the sensitive nature of information rather than whether it is location-based would expand *Carpenter*'s scope–specifically, to commercial DNA information.

III. REEVALUATING THE THIRD-PARTY DOCTRINE'S APPLICATION TO DNA FROM COMMERCIAL DATABASES

It is nearly impossible to function in this modern era of digital communication without sharing a great deal of information with third parties. Third-party services control most aspects of modern life, like communication, finances, school, and the internet, and it is an impractical and unattainable task for an individual to live without sharing private information. *Miller* and *Smith* come from a time-period where voluntary relinquishments of personal information were a significant departure from the norm. In the 1970s, most people kept

114. *Id*. at 2221.

115. *Id*. at 2222.

116. *Id*. at 2220.

117. Paul Ohm, *The Broad Reach of Carpenter v. United States*, JUST SECURITY (June 27, 2018), https://www.justsecurity.org/58520/broad-reach-carpenter-v-united-states/.

their private information private. Now, basically everything the average person does exposes their information under the traditional third-party doctrine. This should lead the judicial system to reexamine whether "voluntariness" and "awareness" of privacy relinquishment are related.

The traditional application of the third-party doctrine was logical a few decades ago, when it was not necessary to share information on such a wide-scale level to participate in society. Back then, it was presumed that when information was given away, the person sharing the information was aware their privacy was lessened. However, people today understand their privacy in terms of privacy settings and policies associated with Facebook and other social media and apps. Although social media users still desire privacy from government intrusion, Pew reported that nearly 70 percent of users do not trust that social media sites will keep their information secure.[118] In a different survey, 80 percent of law enforcement officials reported using social media to further investigations.[119] Although the legal implications of sharing information remain the same, people's understanding of their privacy rights has significantly changed. Most Americans are extremely concerned with keeping their digital information private and controlling how their information is shared.[120] According to the Pew Research Center, 91% of adults believe consumers have no control over how their information is used and transmitted by companies.[121] If people are this concerned about protecting their Facebook "likes" and Twitter posts, then the concept of protecting DNA information should be even more important.

Although the *Carpenter* opinion does not expressly mention DNA, DNA and cell phone data are both private sources of information that

118. Mary Madden & Lee Raine, *Americans' Attitudes About Privacy, Security, and Surveillance*, PEW RES. CTR. (May 20, 2015), www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

119. TheBestVPN LTD., *Can the Police Use Facebook to Investigate Crimes*, GOV'T TECH. (Mar. 5, 2017), www.govtech.com/public-safety/can-the-police-use-facebook-to-investigate-crimes.html.

120. Lee Raine, *The State of Privacy in Post-Snowden America*, PEW RES. CTR. (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/.

121. *Id*. ("Fully 91% of adults agree or strongly agree that consumers have lost control of how personal information is collected and used by companies").

deserve ample protection under the Fourth Amendment. The main difference between the third-party presence in cell phone location and DNA information is the level of voluntary relinquishment. Sharing information with cell phone providers is required to use a cell phone, and cell phones are an essential technology. Further, the average cell phone user is unaware that cell phone towers constantly track their location. However, when it comes to DNA services, the user knowingly decides to purchase an optional service where they opt to provide their genetic information. The third-party doctrine's rationale is better served when there are realistic opportunities to *choose* whether to share information. However, in situations where there is *no choice*, people are backed into a corner. Cell phones are an examples of this because "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[122] As a result, consumers are left unprotected from third-party providers' data use, because user agreements are ill-understood and terms are included in contracts that most users do not read.

Another distinction between *Carpenter* and DNA databases rests on the type of information being exposed. *Carpenter* analyzes physical location information,[123] whereas DNA does not reveal location data on its own. DNA may reveal information about the organic makeup of an individual, but unlike cell phone location data, DNA will not notify the police if an individual is present in a certain state. However, DNA has the potential to enhance location technology. For example, if police investigate a person's DNA through a Snapshot and rely on the facial sketch to search street camera footage, the DNA would help pinpoint a person's location. This reflects how DNA information and conventional surveillance technologies can be used in tandem to gather information previously not available. As these technologies begin to merge, it will eventually become arbitrary to define different types of technology under the law.

Currently, DNA services are not as integral to police investigations as cell phone providers, but they still contain highly sensitive information. As such, the ideology behind *Carpenter* should extend to

122. Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).
123. *Id*. at 2217.

sensitive information like DNA.[124] Genetic information is significantly more sensitive than location-based data provided by cell towers and should require more invasive procedures to access. Regardless of whether DNA data is given knowingly or voluntarily, DNA contains intimate information and functions as a physical map to the human body. The Supreme Court recognizes the sensitive nature of cell phone location data; therefore, this rationale should be extended to other equally or more sensitive information, such as DNA. The third-party doctrine has already been challenged with high level privacy concerns. Therefore, the issues presented in the *Carpenter* case confirm the third-party doctrine has overstretched its intended bounds in the digital age. As Justice Sotomayor has previously declared, "the third-party doctrine is ill suited to the digital age."[125]

The *Carpenter* court acknowledged that cell phone tracking devices are continuing to evolve in "depth, breadth, and comprehensive reach" and the protections of the Fourth Amendment should not be diluted in light of these continued technological advancements.[126] This idea is paralleled with the advancement of DNA use. From individual matches to phenotyping, the versatility of DNA is on the edge of a revolution. The use of DNA data will continue to become even more accurate a few years from now. Although improvements are generally seen as a positive direction, DNA technology is improving at the cost of privacy. Permitting companies to share private information without the user's complete knowledge, via the third-party doctrine, allows companies to aggregate a larger database. In turn, the government is accessing these databases without the need for a warrant.

The evolution of case law in this area exemplifies how the expectation of privacy in the *Katz* case has influenced and transformed privacy law over time. Since advances in technology make it easier to invade privacy, courts have responded in ways to preserve the intent of the Fourth Amendment.[127] The Court's rationale in *Katz* introduced the

124. *See* Levey, *supra* note 96 (finding that "[r]apid technological change inevitably outpaces the glacial evolution of the law and the Carpenter case is a perfect example").

125. Lynch, *supra* note 101.

126. *Carpenter*, 138 S. Ct. at 2223.

127. *See generally* Riley v. California, 573 U.S. 373 (2014) (ruling on the application of the Fourth Amendment to cell phones); *see also* Kyllo v. United States,

general principle that police cannot conduct searches that violate a reasonable expectation of privacy.[128] However, in the decades to follow, police started using new technology to get the same information that was once unavailable because it required a search. Then, in 2001, the Court in *Kyllo* prohibited law enforcement from using sense-enhancing technology to gather information that would otherwise require a physical search to prevent police circumventing searches with technology.[129] This exemplifies how technological advancements can threaten core Fourth Amendment protections. The third-party doctrine needs to account for the sensitive nature of DNA and limit police access to commercial DNA databases by refining its application, just as the Supreme Court in *Kyllo* refined Fourth Amendment jurisprudence to prevent abuse of new technologies.

The Court's rationale in *Kyllo* and *Carpenter* highlights the need for change as technology continues to create new privacy concerns. When technology begins to supersede the controlling law, the law must adapt. Privacy law has adapted to technological advancements before.[130] An established legal principle, present in a completely new and different era from which it was created, requires readjustment to restore balance. Matching the intent of the law with modern ideals is like a pendulum, swinging one way then the opposite until it lands balanced in the middle. The third-party doctrine was created in a time where precise tracking technology was unimaginable. As recently as 2012, "society's expectation has been that law enforcement agents and others would not–and indeed, in the main, simply could not secretly monitor and catalogue every single movement of an individual's car for a very long period."[131] The precision of current technology requires a narrowing of the third-party doctrine.

533 U.S. 27 (2001) (ruling on the application of the Fourth Amendment to thermal imaging devices and other "sense-enhancing" technology).

128. Katz v. United States, 389 U.S. 347, 353 (1967).

129. *Kyllo*, 533 U.S. at 40.

130. *See, e.g.*, *Riley*, 573 U.S. at 385; *see also Kyllo*, 533 U.S. at 40.

131. United States v. Jones, 565 U.S. 400, 430 (2012) (Sotomayor, J., concurring).

IV. THE FUTURE OF DNA PRIVACY

Access to DNA databases enhances police investigatory tactics by increasing the number of available samples to test against evidence. The DNA data from commercial DNA websites can be used to incriminate users, and police have an easier time accessing this data because of the public's interest in finding out about their heritage through DNA testing. With more samples, police could potentially track down more criminals, and increase safety, through direct matches, familial matches, and predicted facial sketches. Proponents of these investigatory methods believe that reduced privacy is a justified sacrifice for protection against crime. But just how far will this tradeoff go? Dr. Thomas May, professor at Washington State University, warns that without laws to make DNA companies more uniform in privacy protections, the customers will inadvertently pay the price.[132]

> . . . regulatory oversight is needed to ensure the privacy of genetic information, determine who should be allowed to submit someone else's sample for testing and for what purposes, and guide the drawing of inferences from DNA results and the relaying of information to persons other than the DNA source who may be implicated by those results — but may be unaware that testing relevant to them has even occurred.[133]

Finding a balance between the benefits DNA websites offer while maintaining some level of individual control over privacy is a solution legislation can provide. According to Senator Charles Schumer, an avid proponent of increasing DNA privacy, consumers are unaware of the underlying rights they give up when signing up for commercial DNA services.[134] Senator Schumer speaks about the dangers unregulated DNA companies pose to privacy, insurance, and employment.[135] Regulating these companies, requiring more transparency about where the user's information is going, and permitting the users to consent to

132. May, *supra* note 77, at 412.

133. *Id*.

134. Shari Logan & Linda Massarella, *Schumer Warns DNA-home Tests Could be Gathering Personal Info*, NY POST, https://nypost.com/2017/11/26/schumer-warns-dna-home-tests-could-be-gathering-personal-info/ (last updated Nov. 26, 2017, 4:03 PM).

135. *Id*.

specific dissemination channels, could provide users with more privacy control. Regulations and transparency are feasible options and many major DNA companies have already modified their privacy statements. These commercial DNA companies are reacting to the public distrust of DNA privacy stemming from the assortment of cases like the Golden State Killer and April Tinsley appearing in mainstream media.[136] However, permitting DNA companies to modify their privacy statements without oversight will lead to inconsistencies in the scope of privacy protection and disclosure. These uneven privacy protections negatively impact consumers, who are not likely capable of understanding the minute differences between the different policy statements to make an educated decision between multiple commercial DNA website options. Instead, consumers might decide which DNA service to purchase based on cost, the testing they want, and other personal preferences. Commercial DNA businesses have demonstrated a willingness to change to protect their customers. However, this change needs to be regulated to ensure customers are evenly protected.

Actions have been set in motion to evaluate the privacy protections in the consumer DNA industry. In 2017, Senator Schumer spoke out about the lack of consumer awareness and rights in the DNA industry:

> When it comes to protecting consumers' privacy from at-home DNA test kit services, the federal government is behind. Besides, putting your most personal genetic information in the hands of third parties for their exclusive use raises a lot of concerns, from the potential for discrimination by employers all the way to health insurance.[137]

In 2018, prompted by Senator Schumer's public endorsement of the issue, the Federal Trade Commission ("FTC") began investigating

136. Since the start of this article, Ancestry.com and other websites have updated their policy statements to include more sections to clarify the privacy rights. *See, e.g.*, *Your Privacy*, *supra* note 73.

137. Press Releases, *Schumer Reveals: Popular at Home DNA Test Kits are Putting Consumer Privacy at Great Risk, as DNA Firms Could Sell your Most Personal Info & Genetic Data to All-Comers; Senator Pushes Feds to Investigate & Ensure Fair Privacy Standards for all DNA Kits*, CHARLES E. SCHUMER (Nov. 26, 2017), https://www.schumer.senate.gov/newsroom/press-releases/schumer-reveals-popular-at-home-dna-test-kits-are-putting-consumer-privacy-at-great-risk-as-dna-firms-could-sell-your-most-personal-info-and-genetic-data-to-all-comers-senator-pushes-feds-to-investigate_ensure-fair-privacy-standards-for-all-dna-kits.

Ancestry.com, 23andMe.com, and other DNA companies to determine if their methods are appropriate.[138] The FTC will determine whether the companies have privacy standards that obtain the full consent of their customers.[139] According to privacy attorney Joel Winston, if the companies are not providing enough disclosure to customers, the "FTC would be expected to prohibit the company form using, sharing, or selling any such DNA data in its possession."[140]

An enforcement action by the FTC would send a clear message that for-profit companies cannot use the fine print to quietly take an ownership interest in their customers' DNA. Companies must not be permitted to mislead, deceive, or confuse customers about how their DNA data is being collected, analyzed, and monetized. Reacting to Senator Schumer, Leslie Fair, a Senior Attorney for the FTC's Bureau of Consumer Protection, warns that these companies' "out-of-the-box defaults" are not very private, and consumers should take an active role in selecting the specific privacy settings they wish to have.[141]

Currently, there are a few laws indirectly protecting genetic privacy. The most recognized law is the Genetic Information Nondiscrimination Act ("GINA"), which was passed in 2008.[142] GINA is designed to protect against civil discrimination in both insurance and employment.[143] Privacy professor Dr. May is optimistic that future

138. Marcus Baram, *The FTC is Investigating DNA Firms like 23andMe and Ancestry over Privacy*, FAST COMPANY (June 5, 2018), https://www.fastcompany.com/40580364/the-ftc-is-investigating-dna-firms-like-23andme-and-ancestry-over-privacy.

139. *See id*. (noting The FTC is investigating "policies for handling personal info and genetic data, and how they share that info with third parties"). "If the FTC finds that any DNA testing company has failed to obtain the full, informed consent of its customers, then the FTC would be expected to prohibit the company" from accessing this type of information. *Id*.

140. *Id*.

141. Chris Brook, *FTC Investigating how DNA Testing Firms Protect User Data*, DIGITAL GUARDIAN (June 11, 2018), https://digitalguardian.com/blog/ftc-investigating-how-dna-testing-firms-protect-user-data.

142. *Genetic Information Discrimination*, U.S. EQUAL EMP. OPPORTUNITY COMMISSION, https://www.eeoc.gov/laws/types/genetic.cfm (last visited May 1, 2019).

143. *Id*.

legislation will enhance the protections that GINA provides.[144] "GINA is a statement by our society that we recognize something's needed – we don't approve of the use of these materials in this way."[145] Dr. May does not believe that GINA is enough to protect people on all sides of the DNA discussion.[146] GINA mainly focuses on civil issues and leaves the burden of proof on the injured party. Dr. May believes that although GINA does not afford significant protections, it shows that society recognizes a need for protection.[147] The mere fact that GINA exists shows that citizens are concerned with protecting their DNA privacy.

The *Carpenter* decision, which requires warrants to obtain cellular location information, is one step towards protecting privacy. The judicial system should continue expanding upon this modern interpretation of "expectation of privacy," as it relates to various digital technologies. Applying the *Carpenter* principle will enhance DNA protection and privacy by preventing this type of information from being accessed without a warrant under the third-party doctrine. The Court in *Carpenter* narrowly decided to exclude cell tower location-based data from the third-party doctrine's scope. Although this case specifically exempted location-based technology, the same principle should be extended to commercial DNA websites. Some scholars view the holding in *Carpenter* as foreshadowing the eventual eradication of the third-party doctrine.[148] "With *Carpenter*, the third-party is almost dead."[149] Although the *Carpenter* decision carved out a narrow exception to the third-party doctrine, privacy expert Paul Ohm comments that the ruling is not technology specific.[150] Rather, the Supreme Court focused on the *nature* of the information. Applying this framework, *Carpenter* could apply to other "information that can locate people."[151]

144. Telephone Interview with Dr. Thomas May, Professor, Wash. State Univ. (Aug. 2, 2018).
145. *Id*.
146. *Id*.
147. *Id*.
148. Ohm, *supra* note 117.
149. *Id*.
150. *Id*.
151. *Id*.

CONCLUSION

DNA is a piece of information dancing on the line between commercial entertainment and medical information. Before these websites existed, visiting a doctor was the only way to access DNA information. The medical field has significant protections in place to keep information safe, but the same cannot be said for these commercial DNA websites. Police should be required to obtain a warrant when seeking DNA from a third-party database. Although this might impair police investigations, it is the price to pay to ensure some level of privacy at the microscopic level. A warrant requires a showing of probable cause, which ensures privacy is not invaded without a legitimate concern for public safety. The *Carpenter* ruling has opened the door for courts to experiment and create broader exceptions to the third-party doctrine. Over the next decade, different types of technology will test the limits of the third-party doctrine. As a result, the third-party doctrine may become obsolete in our digital age. Regardless of how future courts apply *Carpenter*, "the police should think twice before trying to collect . . . [information] without a warrant."[152]

Modification of the third-party doctrine is pivotal to the privacy rights consumers have over their DNA. The rise in commercial DNA websites for recreational purposes challenges the privacy expectations usually associated with one's living organic code. A person shares their sensitive DNA information as soon as they swab their cheek and send their DNA to Ancestry.com or other websites. This technology has the potential to improve and contribute to public safety. However, until such accuracy and privacy can be assured, there are great concerns about DNA databases. "[I]t's easy to say that if things represent threats to privacy we shouldn't allow them. I think that's a little too rash, as there's a lot of good that comes from that testing as well."[153] Legislation that balances the benefits of this technology, while fostering awareness and privacy, will enable shared genetic information to be productive and protective. "What we need is experts in privacy

152. *Id*.
153. Telephone Interview with Dr. Thomas May, *supra* note 144.

technology, geneticists, and law to get together to arrive at a solution."[154]

*Rebecca Gold**

154. *Id*.

* J.D., cum laude, California Western School of Law, 2019; B.A., California Lutheran University, 2016. I would like to thank Professor Robert DeKoven for inspiring this topic and Professor Art Campbell for his editorial feedback and assistance. Special thanks to the *California Western Law Review* staff for their hard work on this piece, and to my sister, Sara, for her additional review and encouragement.