RUTGERS UNIVERSITY LAW REVIEW

VOLUME 72 | ISSUE 2 WINTER 2019

KEEP YOUR FAMILY CLOSE AND YOUR DNA EVEN CLOSER: PROTECTING DNA PRIVACY EXPECTATIONS AFTER *CARPENTER V. UNITED STATES*

*Alexis Smith**

TABLE OF CONTENTS

I. INTRODUCTION

In recent years, the popularity of Direct-to-Consumer ("DTC") testing has exploded.[1] Since 2013, the industry has increased ten-fold and is

* J.D. Candidate, Rutgers Law School, May 2020. A thank you to Professor Adnan Zulfiqar for his guidance, as well as sparking the inspiration for this Note during Criminal Procedure: Investigations. Thank you to all the members of the *Rutgers University Law Review* for their time and efforts during the editorial process. Finally, I want to sincerely thank my parents and those close to me for their unrelenting support and encouragement along the way.

1. Razib Khan & David Mettelman, *Consumer Genomics Will Change Your Life, Whether You Get Tested or Not*, 19 GENOME BIOLOGY 1, 1 (2018), https://genomebiology.biomedcentral.com/track/pdf/10.1186/s13059-018-1506-1.

expected to increase another ten-fold by 2021.[2] Paired with the rise in DTC testing kits is law enforcement's use of these very same databases to solve decades-old crimes.[3]

While catching infamous criminals such as the Golden State Killer is appealing, privacy implications have been generally ignored in the process. As a result of the popularity of these DTC genetic databases, nearly 90% of Americans of European descent will be identifiable through the use of long-range familial matches within the next two to three years.[4]

Due to the lack of statutory privacy protections for DTC genetic testing companies, the United States Supreme Court decision in *Carpenter v. United States*[5] may provide an avenue for protection, especially when paired with the third-party consent and closed container doctrines. This Note will discuss the intersection of genetic testing privacy concerns and Fourth Amendment jurisprudence, as well as advocate the extension of Fourth Amendment protections through *Carpenter*, the closed container doctrine, and the third-party consent doctrine.

II. BACKGROUND

Some of the most sensitive data is genetic information. Unlike credit card numbers or email addresses, genetic information is immutable.[6]

2. *Id.* As of April 2018, fifteen million consumers have completed DTC genetic testing. Yaniv Erlich et al., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 392 SCIENCE 690, 690 (2018). That number increased to twenty-six million by the beginning of 2019. Antonio Regalado, *More than 26 Million People Have Taken an At-Home Ancestry Test*, MIT TECH. REV. (Feb. 11, 2019), https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/.

3. In 2018 alone, one genetic laboratory made twenty-three successful DNA identifications that solved cold cases. Emily Shapiro, *'I Wasn't Sure We Would Ever Find Out': How DNA, Genetic Genealogy Made 2018 the Year to Crack Cold Cases*, ABC NEWS (Dec. 29, 2018, 12:16 PM), https://abcnews.go.com/US/find-dna-genetic-genealogy-made-2018-year-crack/story?id=59367684.

4. Heather Murphy, *Most White Americans' DNA Can Be Identified Through Genealogy Databases*, N.Y. TIMES (Oct. 11, 2018), https://www.nytimes.com/2018/10/11/science/science-genetic-genealogy-study.html?module=inline (citing Erlich et al., *supra* note 2).

5. 138 S. Ct. 2206 (2018).

6. *See* Jennifer Cacchio, *What You Don't Know Can Hurt You: The Legal Risk of Peering into the Gene Pool with Direct-to-Consumer Genetic Testing*, 87 UMKC L. REV. 219, 226 (2018); Angela Chen, *Why a DNA Data Breach Is Much Worse than a Credit Card Leak*, VERGE (June 8, 2018), https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics.

While genetic information is immutable and inherently sensitive, consumers eagerly submit DNA samples to DTC genetic testing companies.[7]

Simultaneously, law enforcement is utilizing the data submitted to DTC testing companies to solve decades-old cases through the practice of long-range familial searches.[8] To solve a case with long-range familial searches, an unidentified DNA sample from the perpetrator of the unsolved crime is entered into a genealogy database.[9] Using the unidentified DNA sample, the family tree is constructed in reverse by compiling a list of relatives spanning to third cousins and then tracing common ancestors back to great-great-grandparents.[10] Missing relatives in the family tree are accounted for using publicly available information, such as obituaries and social media.[11] The family tree is next narrowed to individuals who match the parameters of the suspected perpetrator of the unsolved crime.[12] This process is all completed *before* a search warrant is issued.[13] This information is sometimes used to obtain a warrant for a DNA sample of the familial match in order to compare the crime scene DNA.[14]

While consumers submit genetic samples to DTC genetic testing companies, there is very little statutory protection for this genetic

7. *See* Cacchio, *supra* note 6, at 219.

8. Erlich et al., *supra* note 2. Recently FamilyTreeDNA has even marketed itself as a tool utilized by the F.B.I. to help solve cold cases. Heather Murphy, *Sooner or Later Your Cousin's DNA is Going to Solve a Murder*, N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/us/golden-state-killer-dna.html.

9. Kate Snow & Jon Schuppe, *'This Is Just the Beginning': Using DNA and Genealogy to Crack Years-Old Cold Cases*, NBC NEWS (July 18, 2018, 4:30 AM), https://www.nbcnews.com/news/us-news/just-beginning-using-dna-genealogy-crack-years-old-cold-cases-n892126.

10. *Id.*

11. *Id.*

12. *Id.* In most cases, law enforcement hires a genetic genealogy company such as Parabon NanoLabs to complete the genealogy to produce the narrow list of suspects. *Id.*

13. *See* J.W. Hazel et al., *Is It Time for a Universal Genetic Forensic Database?*, 362 SCI. 868, 898–99 (2018). Often, the narrow list produced by the genetic genealogy company is used to focus surveillance on a particular suspect to collect a DNA sample. Junior Gonzalez, *How They Got Rowe: Pitch from DNA Firm Was 'Last Shot' to Crack Mirack Killing*, LANCASTERONLINE (Jan. 9, 2019), https://lancasteronline.com/news/local/how-they-got-rowe-pitch-from-dna-firm-was-last/article_60e9b516-798b-11e8-8476-eb19e2a7d215.html; Heather Murphy, *Technique Used to Find Golden State Killer Leads to a Suspect in 1987 Murder*, N.Y. TIMES (May 18, 2018), https://www.nytimes.com/2018/05/18/science/ancestry-site-arrest-washington.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.

14. *See* Katherine Kwong, *Third-Party Services as Potential Sources for Law Enforcement Procurement of Genomic Data*, 15 CAN. J.L. & TECH. 99, 101 (2017).

information.[15] Under the Health Insurance Portability and Accountability Act ("HIPAA"),[16] DTC genetic testing companies are not regulated under the privacy rule because the companies are not currently considered "covered entities."[17] Even if DTC genetic testing companies fit within the covered entities definition, an exception in the privacy rule allows for the disclosure of medical information for law enforcement purposes as long as it is pursuant to a "judicial process."[18]

To encourage genetic testing for health purposes, the federal government enacted the Genetic Information Nondiscrimination Act ("GINA").[19] GINA prohibits discrimination in employment and health insurance based on genetic testing information.[20] In addition to protection against discrimination, GINA partially amended HIPAA to include "genetic information" as "health information" covered under HIPAA.[21]

Neither HIPAA nor GINA clearly applies to law enforcement's use of genetic information gathered by DTC testing companies.[22] As a result, the protection of this highly sensitive genetic information is limited to the privacy policies and ethical obligations of the DTC genetic testing companies.[23] Companies such as Ancestry and 23andMe maintain strict privacy policies when handling the disclosure of genetic information to law enforcement.[24] To expand transparency and respond to privacy

15. Natalie Ram et al., *Genealogy Databases and the Future of Criminal Investigation*, 360 SCI. 1078, 1078–79 (2018); *see also* Cacchio, *supra* note 6, at 235–43.

16. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936. HIPAA established the standards of privacy protections afforded to health information. Among other protections, the privacy rule requires covered entities to gain patient authorization before using and/or disclosing health information. 45 C.F.R. § 164.512(i) (2016). The HIPAA privacy rule only applies to "covered entities." 45 C.F.R. § 164.306(a) (2016).

17. Ram et al., *supra* note 15, at 1078. "Covered entities" include healthcare providers and healthcare insurance companies. *See* 45 C.F.R. § 164.306(a) (2016).

18. *See* Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1384 (2019) (citing 45 C.F.R. § 164.512(f) (2016)).

19. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110–233, 122 Stat. 881.

20. *Id.* at 893–96 (codified as amended at 42 U.S.C. § 300gg-52 (2018)); *id.* at 907–08 (codified as amended at 42 U.S.C. § 2000fff-1 (2018)).

21. *Id.* at 903–05 (codified as amended at 42 U.S.C. § 1320d–9 (2018)).

22. *See* 45 C.F.R. § 164.104, .306(a), .512(i) (2016).

23. *See id.*

24. Ancestry's privacy policy states that the company will only disclose personal and genetic information to law enforcement if the company believes it is "reasonably necessary" to "[c]omply with [a] valid legal process (e.g., subpoenas, warrants)." *Your Privacy*, ANCESTRY, https://www.ancestry.com/cs/legal/privacystatement (last updated Dec. 23, 2019). In the case that Ancestry discloses information to law enforcement, Ancestry

concerns,[25] both Ancestry and 23andMe now publish annual transparency reports that outline the number of requests and fulfilled requests made by law enforcement.[26] On the other hand, GEDMatch[27] and FamilyTreeDNA[28] seem to encourage use by law enforcement.[29]

In addition to the concerns surrounding law enforcement's use of genetic information without a search warrant, genetic testing companies reserve the right to share the anonymized genetic information for research purposes and drug development.[30] As recently as July 2018, 23andMe and GlaxoSmithKline entered into a $300 million deal[31]

provides notice if possible. *Id.*; *see also Ancestry Terms and Conditions*, ANCESTRY, https://www.ancestry.com/cs/legal/termsandconditions#ContentUsed (last updated July 25, 2019). 23andMe has similar protections, with its privacy policy stating: "*We will not* provide information to *law enforcement* or *regulatory authorities* unless required by law to comply with a valid court order, subpoena, or search warrant for genetic or Personal Information." *Privacy Highlights*, 23ANDME, https://www.23andme.com/about/privacy/ (last updated Jan. 1, 2020).

25. After the headline-grabbing case of Michael Ursy, Ancestry changed its genetic database to non-public. Michael Usry's father submitted a DNA sample to a non-profit program, which was later purchased by Ancestry. Ancestry subsequently made the genetic data publicly available. Law enforcement found a strong genetic match in the database to DNA found at the scene of an unsolved crime. Law enforcement utilized that match, in combination with information from Facebook, to obtain a search warrant for a DNA sample from Michael Usry for comparison purposes. Michael Ursy's DNA did not match the DNA found at the crime scene. Ancestry changed the databases to non-public in response to the major headlines. Kwong, *supra* note 14, at 101–02.

26. In 2017, Ancestry fulfilled thirty-one of thirty-four law enforcement requests for personal information. *Ancestry 2017 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency (last visited Jan. 9, 2019). In 2018, Ancestry fulfilled seven of the ten requests. *Ancestry 2018 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency (last visited Dec. 27, 2019). As of October 15, 2019, 23andMe has received seven law enforcement requests, none of which it fulfilled. *23andMe Transparency Report*, 23ANDME, https://www.23andme.com/transparency-report/ (last visited Dec. 27, 2019).

27. GEDMatch is different than Ancestry and 23andMe. GEDMatch is a public database where individuals with test results from a DTC genetic company can upload the raw genetic data. *See GEDMatch.com Terms of Service and Privacy Policy*, GEDMATCH, https://www.gedmatch.com/tos.htm (last updated Dec. 9, 2019).

28. FamilyTreeDNA explicitly supports use by law enforcement through law enforcement accounts. Users may opt-out of the law enforcement matching system. *FamilyTreeDNA Privacy Statement*, FAMILYTREEDNA, https://www.familytreedna.com/legal/privacy-statement (last updated May 7, 2019); *see also* Murphy, *supra* note 8.

29. Ram, *supra* note 18, at 1363–64. An authorized use of the data under the terms and privacy policy is "[f]amilial searching by third parties such as law enforcement agencies to identify the perpetrator of a crime, or to identify remains." *GEDMatch.com Terms of Service and Privacy Policy*, *supra* note 27.

30. Cacchio, *supra* note 6, at 224–25.

31. This is not unique. Even before the 2018 GlaxoSmithKline agreement, 23andMe has published studies with Pfizer, Janssen, and GlaxoSmithKline. Sarah Zhang, *Big*

granting GlaxoSmithKline access to 23andMe's anonymized and aggregated genetic database.[32]

These agreements between genetic testing companies and pharmaceutical companies are cause for concern.[33] First, the federal government launched a campaign to create a genetic database for research purposes.[34] Presently, the campaign encourages anyone over the age of eighteen to submit their DNA through the website or participating healthcare providers.[35] This campaign seems innocuous at first glance, but the submitted data remains in the database indefinitely and illustrates the federal government's desire to build a genetic database.[36] While the desire is currently to advance medical research, the growing success of long-distance familial searches to solve crimes may encourage the government to move towards a universal genetic forensic database.[37] The willingness of DTC genetic testing companies to sell data, paired with minimal legal protections, makes it a real possibility that these companies will sell genetic data to the government for the right price.[38]

Another cause for concern is hacking. MyHeritage, one of the smaller DTC genetic testing companies, experienced a data breach of ninety-two million accounts.[39] Veritas also experienced a security breach in 2019.[40] While neither breach included genetic data, the incidents suggest a future of hacking attempts as the DTC genetic testing industry continues

Pharma Would Like Your DNA, ATLANTIC (July 27, 2018), https://www.theatlantic.com/science/archive/2018/07/big-pharma-dna/566240/; *see also* Denise Roland, *How Drug Companies Are Using Your DNA to Make New Medicine*, WALL ST. J. (July 22, 2019), https://www.wsj.com/articles/23andme-glaxo-mine-dna-data-in-hunt-for-new-drugs-11563879881?mod=searchresults&page=1&pos=3.

32. Zhang, *supra* note 31; *see also* Ram, *supra* note 18, at 1410. 23andMe allows customers to opt out of their genetic profile's use in research. Zhang, *supra* note 31.

33. Cacchio, *supra* note 6, at 225.

34. *U.S. Government Seeking 1 Million People for Study of DNA*, CBS NEWS (May 3, 2018, 10:55 AM), https://www.cbsnews.com/news/u-s-government-seeking-1-million-people-for-study-of-dna-health-habits/.

35. *Id.*

36. Consent for research and data sharing may be withdrawn for use, excluding aggregate datasets, past studies, and studies that already began. *See Precision Medicine Initiative: Privacy and Trust Principles*, NAT'L INST. HEALTH, https://allofus.nih.gov/about/program-overview/precision-medicine-initiative-privacy-and-trust-principles (last visited Jan. 9, 2019).

37. *See* Hazel et al., *supra* note 13, at 898.

38. Part of the business model of 23andMe was to eventually sell data for research purposes. Zhang, *supra* note 31.

39. Chen, *supra* note 6; *see supra* notes 1–3 and accompanying text.

40. Kristen Brown, *Breach at DNA-Testing Firm Veritas Exposed Customer Information*, BLOOMBERG (Nov. 6, 2019), https://www.bloomberg.com/news/articles/2019-11-06/breach-at-dna-test-firm-veritas-exposed-customer-information.

to grow.[41] Data breaches by large companies are not unheard of. In 2017, hackers accessed the Equifax database.[42] Social security numbers, driver's license numbers, and other personal information of 143 million Americans were possibly compromised in the breach.[43] Even though DTC genetic testing companies anonymize the information for storage and sale, the data can be de-anonymized by a lay person through the use of GEDMatch and other public genetic tools.[44] Once the data is de-anonymized, the inherently sensitive and immutable genetic information may be distributed and used for purposes such as insurance discrimination or identity theft.[45]

III. FOURTH AMENDMENT PROTECTIONS AND THE SUPREME COURT'S RESPONSE TO TECHNOLOGICAL ADVANCEMENTS

While there are nearly no statutory protections for DNA gathered from DTC genetic testing companies for law enforcement purposes, this process creates significant Fourth Amendment implications. The Fourth Amendment protects an individual against unreasonable searches and seizures of their person, houses, papers, and effects.[46] For searches of these protected spheres, a warrant must typically be issued.[47] A valid warrant under the Fourth Amendment must be approved by a neutral magistrate, supported by probable cause, limited in scope, and made with sufficient particularity as to the place, persons, and objects to be searched.[48] Any warrantless search of a protected activity or object is per se unreasonable unless an exception applies.[49]

For an activity or object to be protected under the Fourth Amendment, the *Katz* test requires a reasonable expectation of privacy.[50] A reasonable expectation of privacy must be both subjectively and objectively reasonable.[51] An individual must exhibit an actual expectation of privacy for the subjective prong, while the objective prong requires society to deem the expectation of privacy reasonable.[52]

41. Chen, *supra* note 6; Khan & Mettelman, *supra* note 1.
42. Equifax is a credit reporting agency. Cacchio, *supra* note 6, at 238.
43. *Id.*
44. *Id.* at 231; Erlich et al., *supra* note 2, at 693.
45. *See* Cacchio, *supra* note 6, at 233; Chen, *supra* note 6.
46. U.S. CONST. amend. IV.
47. *Id.*
48. *Id.*
49. Katz v. United States, 389 U.S. 347, 357 (1967).
50. *See id.* at 360 (Harlan, J., concurring).
51. *Id.* at 361.
52. *Id.*

The Supreme Court has struggled in extending Fourth Amendment privacy protections with the explosion of technological developments in recent decades.[53] Rather than applying the *Katz* expectation of privacy test, the Court has avoided the reasonableness analysis by extending Fourth Amendment protections through the traditional trespass test.[54]

IV. *CARPENTER V. UNITED STATES*: THE SUPREME COURT'S (PARTIAL) RESOLUTION OF TECHNOLOGICAL PRIVACY CONCERNS

The Supreme Court recently illustrated a shift from avoiding technological privacy expectations to tackling the issue head-on in *Carpenter v. United States*.[55] The Court ruled the compulsory request to turn over cell-site location information ("CSLI") through a court order under the Stored Communications Act ("SCA") constituted a search that violated the Fourth Amendment.[56] The compulsory request violated the Fourth Amendment because an individual maintained a reasonable expectation of privacy in their physical movements recorded by a cell phone, even when that location data was stored with a third-party cellular provider.[57]

In *Carpenter*, one of four arrested suspects confessed and identified fifteen accomplices to a string of robberies.[58] Pursuant to the SCA,[59] federal agents applied for two court orders to compel the CSLI from the wireless providers of Carpenter, one of the named accomplices who

53. *See, e.g.*, Riley v. California, 573 U.S. 373, 400–03 (2014) (deciding a search through an arrestee's cell phone during a search incident to arrest was unreasonable and required a warrant); United States v. Jones, 565 U.S. 400, 412 (2012) (ruling the placement of a GPS device on a vehicle for 28 days was a search because it was a physical intrusion without a valid warrant); Kyllo v. United States, 533 U.S. 27, 34–35, 40 (2001) (ruling the warrantless use of a thermal imaging device from the street to detect heat emanating from a home was a search because it explored details of the home that would not have been accessible without this technology or physical intrusion); United States v. Warshak, 631 F.3d 266, 287–88 (6th Cir. 2010) (ruling the warrantless compulsion to turn over emails violated the Fourth Amendment because emails maintain the same expectation of privacy as letters).

54. *See, e.g.*, *Jones*, 565 U.S. at 412; *Kyllo*, 533 U.S. at 34–35.

55. 138 S. Ct. 2206 (2018); *see Riley*, 573 U.S. at 400–03; *Jones*, 565 U.S. at 412; *Kyllo*, 533 U.S. at 34–35, 40; *Warshak*, 631 F.3d at 287–88.

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

57. *Id.* at 2222–23.

58. *Id.* at 2212.

59. The Stored Communications Act ("SCA") permits the government to compel the disclosure of certain telecommunication 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.'" *Carpenter*, 138 S. Ct. at 2212 (quoting Stored Communications Act, 18 U.S.C. § 2703(d) (2018)).

appeared in the call records of the cooperating suspect.[60] With the location data placing Carpenter in the vicinity of the robberies at the corresponding times, Carpenter was arrested, subsequently convicted on all six counts of robbery, and sentenced to more than 100 years in prison.[61]

Beginning with original intent, the Court examined the two guideposts of Fourth Amendment privacy protection analysis.[62] Fourth Amendment protections are intended to safeguard "'the privacies of life' against 'arbitrary power'" and "to place obstacles in the way of a too permeating police surveillance."[63] With that backdrop, the Court discussed the intersection between the expectation of privacy in physical movements and the information shared with a third party.[64] When an individual shares information with a third party, the individual has no expectation of privacy because the individual assumes the risk of disclosure by the third party.[65]

In deciding *Carpenter*, the Court refused to apply the third-party doctrine to CSLI.[66] As a result, the warrantless search of the data was per se unreasonable because the individual maintained a reasonable expectation of privacy.[67]

The Court reasoned that there is a reasonable expectation of privacy with regard to CSLI by comparing the case to the GPS monitoring at issue in *United States v. Jones*.[68] Just because the CSLI was held by the third-party cellular provider, it did not automatically negate a reasonable privacy expectation in such sensitive data.[69] The Court explained that CSLI is similar to the GPS monitoring data in *Jones* because it illustrates

60. *See id.* The first order requested 152 days of cell-site records from MetroPCS, while the second order sought seven days of CLSA from Sprint. However, produced records included a total of 129 days of phone records and 12,898 location points. *Id.*

61. *Id.* at 2212–13.

62. *Id.* at 2214.

63. *Id.* (first citing Boyd v. United States, 116 U.S. 616, 630 (1886); then citing United States v. Di Re, 332 U.S. 581, 595 (1948)).

64. *See id.* at 2215–16.

65. *Id.* at 2216 (first citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (ruling there is no expectation of privacy to numbers recorded in a pen register since phone numbers are regularly shared with third parties); then citing United States v. Miller, 425 U.S. 435, 443 (1976) (ruling there is no legitimate expectation of privacy when information is given to a third party, even if it was under the assumption that it was for a limited purpose)).

66. *Id.* at 2216–17.

67. *Id.* at 2217–19 (citing United States v. Jones, 565 U.S. 400, 430 (2012)).

68. *Id.*

69. *Id.* at 2217.

intimate details of an individual's life.[70] Additionally, privacy concerns are elevated with CSLI because of the level of precision.[71] In the world we live in today, a cell phone goes everywhere an individual goes, allowing for "near perfect surveillance."[72] Another concern is the level of precision achievable with little to no investment by law enforcement.[73] Using GPS technology or CSLI to obtain extremely sensitive information is significantly cheaper and more efficient than traditional police work.[74] Traditional police work takes time and is often flawed, while cellular records are near perfect for the preceding five years.[75]

The Court further noted that it would be a negative for all individuals who own a cell phone to allow the use of this inherently sensitive data without any Fourth Amendment protections.[76] Without protection, CSLI essentially provides the government near perfect surveillance for the past five years for any possible suspect.[77] To rebut the government's argument that the CSLI did not alone implicate Carpenter,[78] the Court reiterated that an inference does not insulate the search from Fourth Amendment protections.[79] Even though the CSLI in *Carpenter* was accurate to between one-eighth to four square miles, more precise technology is already in use or development, and the Court must take account of such advancements.[80]

After deciding the government's warrantless search of CSLI invaded a reasonable expectation of privacy, the Court explained the inapplicability of the third-party doctrine.[81] Under the third-party doctrine, an individual does not have a legitimate expectation of privacy in information voluntarily shared with another.[82] Unlike regular third-party witnesses,[83] the information CSLI obtained from cellular providers was extremely accurate and acted as an infallible memory.[84]

70. *Id.* at 2217–18.
71. *Id.* at 2218.
72. *Id.* at 2217–18.
73. *Id.*
74. *Id.*
75. *Id.* at 2218.
76. *Id.*
77. *Id.*
78. *Id.* at 2218 (citing Kyllo v. United States, 533 U.S. 27, 36 (2001)).
79. *Id.*; *see supra* text accompanying notes 62–67.
80. *Carpenter*, 138 S. Ct. at 2218–19.
81. *Id.* at 2219–20.
82. *Id.* at 2216 (first citing Smith v. Maryland, 442 U.S. 735, 743–44 (1979); then citing United States v. Miller, 425 U.S. 435, 443 (1976)).
83. In *Smith*, the third party was a pen register and, in *Miller*, it was bank records held by the bank. 442 U.S. at 737; 425 U.S. at 437–38.
84. *See Carpenter*, 138 S. Ct. at 2219–20.

The Court explained that neither rationales of the third-party doctrine applied to CSLI.[85] The third-party doctrine is based on the idea that there is a reduced expectation of privacy in information voluntarily shared with another.[86] On the contrary, Fourth Amendment protections are not completely void when information is shared with a third party.[87] Application of the third-party doctrine must also consider "'the nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'"[88] The content of CSLI was particularly invasive because it tracked an individual's every move, especially when considering its detail and reliability over a five-year period.[89]

The second primary rationale for the third-party doctrine was also not accomplished. Under the doctrine, the sharing party assumes the risk of exposure when information is shared with a third party.[90] Not only are cell phones an integral piece of everyday life and pervasive among society, the cell phone user took no affirmative action to share the location data with the cellular provider.[91] As a result, the Court refused to extend the third-party doctrine to CSLI since the individual only shared the information with the cellular provider and did not voluntarily assume the risk.[92]

By categorizing the acquisition of CSLI as a search, the information was afforded Fourth Amendment protections.[93] Under Fourth Amendment jurisprudence, searches are only reasonable with a facially valid warrant or an exception to the warrant requirement.[94] In the case of CSLI, the information was acquired through a court order under the SCA.[95] Records can be compelled under the SCA if reasonable grounds can be articulated that the desired information "[was] 'relevant . . . to an ongoing investigation.'"[96] This standard is far below the probable cause standard required for a search warrant.[97] Since the acquisition of CSLI

85. *Id.* at 2219–20.
86. *Id.* at 2219.
87. *See id.*
88. *Id.* (citing *Miller*, 425 U.S. at 442).
89. *Id.* at 2220.
90. *See id.*
91. *Id.* Collection of CSLI took place anytime the cell phone was turned on—the owner did not have to take any affirmative steps to enable/disable the collection of data. *Id.*
92. *Id.*
93. *See id.* at 2221.
94. *Id.*
95. *Id.*
96. *Id. (*citing Stored Communications Act, 18 U.S.C. § 2703(d) (2018)).
97. *Id.* at 2221.

enjoyed a reasonable expectation of privacy, and no warrant, probable cause, or exception to the warrant requirement was present, the Fourth Amendment was violated.[98] Furthermore, when an individual has a reasonable expectation of privacy in records, the government cannot subpoena the records held by a third party.[99]

To conclude the decision, the Court reiterated that the growth of technology should not limit Fourth Amendment protections.[100] The government's warrantless intrusion into such comprehensive data contained in the CSLI was exactly what the Framers sought to protect with the Fourth Amendment.[101]

V. APPLICATION OF *CARPENTER* TO GENETIC DATA STORED WITH DTC GENETIC TESTING COMPANIES

Long-range familial searches through DTC genetic testing companies pose significant Fourth Amendment privacy concerns. *Carpenter* opened the door to recognizing Fourth Amendment privacy protections for genetic information by acknowledging an expectation of privacy in sensitive personal information retained by a third party.[102] In Justice Gorsuch's dissent, he directly discussed the outdated third-party doctrine and the impact on genetic information: "Can it 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."[103]

Genetic information shares many of the same privacy concerns as the CSLI addressed in *Carpenter*.[104] Like the location information gathered through a cell phone by a third-party cellular provider, the DTC genetic information is gathered and stored with the genetic testing company.[105] Genetic information is inherently personal, even more so than location data.[106] While CSLI contains five years of records, DNA on the other hand uniquely identifies an individual and includes immutable genetic health

98. *See id.* at 2221–22.

99. *Id.* The Court recognized that exigent circumstances for a warrantless search are an exception to the general ban on the warrantless acquisition of CSLI. *Id.* at 2222–23.

100. *See id.* at 2223.

101. *See id.*

102. *See* Ram, *supra* note 18, at 1390–1400.

103. *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).

104. *See supra* text accompanying notes 62–78.

105. *See Carpenter*, 138 S. Ct. at 2217; *supra* text accompanying notes 23–26.

106. *See* Cacchio, *supra* note 6, at 223; Ram, *supra* note 18, at 1389–90.

risks, carrier status, ancestry, and traits.[107] Applying the *Katz* reasonable expectation of privacy test to genetic information suggests that an expectation of privacy is both subjectively and objectively reasonable.[108]

As the Court emphasized in *Carpenter* with CSLI, all Fourth Amendment protections are not lost when an individual enters the public sphere and the act or information is intended as private.[109] This is particularly relevant to the genetic information shared with DTC genetic testing companies. Like the location data in *Carpenter* that produced intimate details of an individual's life,[110] genetic information is possibly the most sensitive and intimate personal information available.[111] Genetic information poses an even greater privacy concern than CSLI because of the immutability and insight into an individual's health risks, ancestry, and traits.[112]

Just as acquisition of the CSLI made for extremely efficient and inexpensive police work with near perfect accuracy, the collection of genetic information makes for a much easier, less time-consuming process for law enforcement, with no procedural safeguards of the warrant procedure.

In *Carpenter*, the government unsuccessfully argued that the necessary inference from the location data insulated the search from Fourth Amendment protections.[113] That same argument would also likely be rejected when applied to genetic information. Like the CSLI that did not alone place Carpenter at the crime scenes, the genetic information at issue here is also used alongside traditional police work.[114] Both CSLI and genetic information require an inference made by law enforcement, which suggests similar Fourth Amendment protections for genetic information.[115]

The Court's consideration of more accurate technology already in use or development is also applicable to genetic information. While the CSLI in *Carpenter* was extremely accurate, it was not the most accurate location technology available.[116] Comparing the technology utilized by

107. *See Carpenter*, 138 S. Ct. at 2218; Cacchio, *supra* note 6, at 223.
108. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
109. *Carpenter*, 138 S. Ct. at 2217 (citing *Katz*, 389 U.S. at 351–52).
110. *Id.*
111. *See* Cacchio, *supra* note 6, at 223–24, 236–40; Ram, *supra* note 18, at 1389–90.
112. *See* Cacchio, *supra* note 6, at 222–23.
113. *Carpenter*, 138 S. Ct. at 2218–19.
114. Cacchio, *supra* note 6, at 226–28.
115. *See Carpenter*, 138 S. Ct. at 2218; Cacchio, *supra* note 6, at 226–28.
116. *See supra* text accompanying note 80.

DTC genetic testing companies to that of law enforcement, DTC genetic testing is significantly more precise.[117] State and federal forensic databases analyze forty data points of its DNA samples, while DTC genetic testing companies locate around 600,000 data points.[118] This level of precision in genetic information stored with DTC genetic testing companies is an entirely new species of data that poses greater privacy concerns.[119]

In *Carpenter*, the primary counter-argument was the third-party doctrine.[120] The counter-argument is the same for genetic information submitted to DTC genetic testing companies. It is argued the risk of disclosure is assumed when individuals voluntarily submit DNA samples. For the same reasons the argument was rejected in *Carpenter*, the third-party doctrine is inapplicable to genetic information.

Neither justification for the third-party doctrine was sufficient in *Carpenter* because an individual does not automatically surrender all Fourth Amendment protections when information is voluntarily shared with a third party, nor does the individual assume the risk of disclosure by that third party.[121] Just as with CSLI, the genetic information is voluntarily shared with a commercial third party. Since the only voluntariness by the individual was carrying the cell phone, there was no assumption of risk in CSLI because the collection of the data was automatically collected.[122]

While the level of voluntariness in sharing genetic information is presently greater than in CSLI,[123] the nature of genetic information is significantly more sensitive.[124] Application of the third-party doctrine must consider the nature of the information to determine if there is still

117. Ram, *supra* note 18, at 1378–80. The Court in *Maryland v. King* ruled that taking a DNA sample during the normal arrest procedure is constitutional because the governmental need for identification outweighs the minor intrusion of acquiring a DNA sample during an arrest where the expectation of privacy is diminished. 569 U.S. 435, 464–66 (2013).

118. Ram, *supra* note 18, at 1378–89.

119. In *Carpenter*, the CSLI was significantly more invasive than the GPS information analyzed in *Jones*, which created even greater privacy concerns for CSLI. *Carpenter*, 138 S. Ct. at 2218–20, 2222.

120. *See id.* at 2219.

121. *See supra* text accompanying notes 81–92.

122. The Court stated that CSLI was not "shared" as we normally think. Rather, cell phones are presently indispensable to society and there is no affirmative act by the cell phone owner to enable the collection of CSLI. *Carpenter*, 138 S. Ct. at 2220.

123. Under an Equal Employment Opportunity Commission rule, an employer may penalize an employee for the lack of participation in wellness programs, which sometimes include genetic testing. Cacchio, *supra* note 6, at 236.

124. Cacchio, *supra* note 6, at 223.

a legitimate expectation of privacy since all Fourth Amendment protections are not forfeited by entering the public sphere.[125] The Court reasoned in *Carpenter* that the nature of CSLI was particularly invasive since it provided a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[126]

The genetic information at issue here is significantly more invasive than the location data from *Carpenter*.[127] Genetic information is immutable, precise, and cannot be made confidential again after disclosure.[128] Even though there is more voluntariness in submitting genetic information to commercial companies, the invasive nature of genetic information overshadows the voluntary aspect. While the sharing of CSLI may have been less voluntary than submitting DNA to commercial companies, the immutability and invasive nature of DNA provides significantly greater privacy concerns than five years of location data. As a result, the third-party doctrine should not apply since the inherently sensitive nature of genetic information supports a legitimate expectation of privacy.

Like in *Carpenter*, there should be a reasonable expectation of privacy in genetic information because of the inapplicability of the third-party doctrine. On the other hand, it may be argued that the privacy policies of the DTC testing companies weigh against an objective expectation of privacy.[129] Companies such as Ancestry and 23andMe retain the right to share genetic data, yet the companies stress their reluctance to provide genetic information to law enforcement.[130]

A reasonable expectation of privacy in genetic information has already been discussed by the Supreme Court in *Maryland v. King*.[131] The Court ruled that the swab of an arrestee's cheek for a DNA sample was constitutional because the government's substantial interest in

125. *See supra* text accompanying notes 62–69.

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

127. *See supra* text accompanying notes 110–12.

128. *See* Cacchio, *supra* note 6.

129. Commercial companies often have an "informed consent" section which notifies the individual that the genetic information may be used by law enforcement. Cacchio, *supra* note 6, at 228.

130. *See supra* note 24 and accompanying text. Along the same lines, Ancestry and 23andMe both publish Transparency Reports. *See supra* text accompanying notes 25–26. On the other hand, public databases such as GEDMatch and FamilyTreeDNA that expressly allow for law enforcement's use of the database may have a lesser expectation of privacy. Even for information that is submitted to these databases, there is arguably a reasonable expectation of privacy when considering the inherent sensitivity of the genetic information. *See* Ram, *supra* note 18, at 1381.

131. 569 U.S. 435, 464–65 (2013).

identification of the arrestee outweighed the minimal intrusion of the swab during the routine booking procedure where the expectation of privacy was already reduced.[132] Law enforcement's use of an individual's genetic information satisfies all of the privacy concerns that were not present in *King*.[133] Consequently, it is hard to comprehend that an arrestee's DNA is provided a greater expectation of privacy than the DNA of an individual where the probable cause standard is not established.

Finally, society's treatment of genetic information supports the reasonable expectation of privacy. In addition to GINA, more than half of states have implemented some type of statutory protections for genetic information.[134]

Assuming there is a reasonable expectation of privacy in genetic information held by DTC testing companies, the protections of the Fourth Amendment would apply. Like in *Carpenter* where the acquisition of the CSLI through a court order was insufficient to satisfy the warrant requirement, law enforcement's warrantless acquisition of genetic information is unconstitutional under the Fourth Amendment.

VI. REASONABLE EXPECTATION OF PRIVACY FOR LONG-RANGE FAMILIAL MATCHES

In most cold cases solved with long-range familial matches partially created through genetic databases, the individual who submitted the data was not the individual implicated for the crime.[135] As a result, the privacy considerations are not just limited to the individual who submitted the genetic sample, but also those who are implicated through familial matches.[136] A possible method of ensuring Fourth Amendment privacy protections of long-range familial matches is the application of the third-party consent and closed container doctrines.[137]

132. *See id.* at 465.

133. *See id.* at 464–65. Combined DNA Index System ("CODIS") samples in *King* were only enough for identification and state statutory protections were present. *Id.* Unlike the DNA in question in *King*, the DNA obtained from DTC genetic testing companies contain medical information and lack any statutory protections for the warrantless practice.

134. Ram, *supra* note 18, at 1383; *see also supra* text accompanying notes 19–21 (discussing GINA).

135. *See supra* text accompanying notes 8–12.

136. *See*, *e.g.*, *supra* text accompanying notes 8–12.

137. *See* Ram, *supra* note 18, at 1399–1400. While Ram does propose the possible application of *Carpenter* to provide Fourth Amendment privacy protections to genetic information, Ram does not address or provide a solution to the privacy concerns of familial matches.

A. Crossroads Between the Third-Party Consent and Closed Container Doctrines as Applied to Electronics

Without a warrant, a search is per se unreasonable unless there is an applicable exception.[138] One exception is the third-party consent doctrine.[139] A third party can consent to a search of an individual's property if the individual assumed the risk that the third party may allow a search of the property.[140] To determine if an individual assumed the risk of a consent search, the court must consider the circumstances of the parties' property use to decide whether the third party "possesses common authority" over the property.[141] This analysis includes Fourth Amendment societal expectations of the property.[142] The following factors should be considered: the sensitivity of the property, steps taken by the individual to protect the property from the third party, and foreseeability of the third party exercising authority over the property.[143] These factors and overall considerations are used to determine the reasonableness of the expectation of privacy in the object or activity in question.[144]

In the case of electronic devices, some argue conceptual similarities between privacy expectations in electronic devices and privacy expectations in suitcases or briefcases.[145] Like suitcases or briefcases, electronic devices are "physical items that are associated with strong privacy interests" and have subjective and objective expectations of privacy.[146] *Riley v. California* recognized a reasonable expectation of privacy in cell phones.[147] The Court reasoned that cell phones were a

138. Riley v. California, 573 U.S. 373, 382 (2014).

139. United States v. Matlock, 415 U.S. 164, 171 (1974). The third-party consent search should not be confused with the third-party doctrine established in *Smith/Miller*, discussed *supra* note 83.

140. *Matlock*, 415 U.S. at 171.

141. *Id.* at 170.

142. *See id.* at 171 n.7. A third-party consent search is only permissible "when a person shares property with a third party in a manner that—according to the prevailing social norms—compromises that person's privacy expectation in the property." Kevin Golembiewski, *All Data Are Not Created Equal: Upholding the Fourth Amendment's Guarantees When Third Party Consent Meets the Shared Electronic Device*, 56 WASHBURN L.J. 35, 42, 44–47 (2017) (arguing that in determining the constitutionality of electronic device searches, there should be a reasonableness consideration because all data is not of the same sensitivity).

143. Golembiewski, *supra* note 142, at 42.

144. *Id.*; *see also supra* text accompanying notes 46–52.

145. Golembiewski, *supra* note 142, at 44.

146. *Id.*

147. 573 U.S. 373, 393–97 (2014). While *Riley* did not argue that cell phones maintained a reasonable expectation of privacy because of the closed container doctrine, the government did not explicitly address the argument either. In the decision, the Court did

unique category of effects that required a heightened privacy interest because of the volume of personal information.[148]

Similar to cell phones, emails and digital documents contained within email accounts arguably enjoy Fourth Amendment protection through the application of the closed container doctrine.[149] Like a closed container where the owner takes affirmative steps to shield the contents from the public, the user of an email account takes steps to protect information through password protection.[150] The owner of a closed, locked container is likely the only individual able to access the container, similar to an email account.[151] Even though users are or should be aware that servers such as Google are able to access the email account information, an objectively reasonable expectation of privacy from personal access by employees or law enforcement still remains in the password protected information.[152]

B. Closed Container Doctrines as Applied to Genetic Information

Genetic information held by genetic testing companies shares many of the same characteristics of electronic devices, cell phones, and email accounts.[153] Like the information or objects contained in a closed container or electronic device, genetic information is associated with strong privacy interests.[154] Even though genetic information is not a physical object, it acts as a locked container since it is not the container itself that enjoys an expectation of privacy but the information inside. Furthermore, like cell phones that require a heightened expectation of privacy due to the amount of personal information contained within the device, genetic information contains a vast amount of personal information that provides insight into the most sensitive and personal aspects of an individual's identity.[155] While the phone itself is not

address the government's concession that search incident to arrest cannot likely be extended to information stored on a remote server and accessed through a cell phone. *Id.* at 375. The Court responded that the "possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee is yet another reason that the privacy interests [with cell phones] dwarf" traditional privacy interests. *Id.* at 398.

148. *Id.*; *see also* Golembiewski, *supra* note 142, at 46.

149. Andrew William Bagley, *Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects*, 21 ALB. L.J. SCI. & TECH. 153, 176 (2011).

150. *Id.*

151. *Id.* at 176–77.

152. *Id.* at 176.

153. *See* Cacchio, *supra* note 6, at 223; *supra* text accompanying notes 141–48.

154. *See* Cacchio, *supra* note 6, at 225–26; *supra* text accompanying notes 145–52.

155. *See* Cacchio, *supra* note 6, at 223; Ram, *supra* note 18, at 1386, 1390–91.

intimate property, the information contained inside the cell phone is.[156] This characteristic is similar to genetic information, where anonymized DNA is mildly safe,[157] but once it is de-anonymized and linked to an individual, the information is inherently personal and revealing.[158]

Genetic information is also similar to email and internet accounts. Analogous to closed containers and email accounts, the individual who submitted the genetic information took steps to protect the data through password protection.[159] Closed containers, cell phones, email accounts, and genetic information stored with DTC genetic testing companies are further comparable since only one individual typically has access to the object or account.[160] Finally, like an email account where an individual arguably has an expectation of privacy from possible access by employees and law enforcement,[161] the information held by DTC genetic testing companies should also enjoy a reasonable expectation of privacy, even though the companies reserve the right to share the anonymized data.[162]

C. Third-Party Consent Doctrine, Closed Container Doctrine, and the Tenth Circuit Test as Applied to Genetic Information

Assuming genetic information held by DTC genetic testing companies is constitutionally protected through the closed container doctrine,[163] long-range familial matches may enjoy Fourth Amendment protections with the application of the third-party consent doctrine. The third-party consent doctrine could help determine whether one family member may submit their DNA to a DTC genetic testing company, as well as whether that submission waives the expectation of privacy in the genetic information for family members who did not consent or affirmatively denied consent.[164]

156. *See* Riley v. California, 573 U.S. 373, 386 (2014).

157. It is possible for an individual with proficient internet skills to de-anonymize genetic information. Cacchio, *supra* note 6, at 231.

158. *See* Cacchio, *supra* note 6, at 223; Ram, *supra* note 18, at 1379–81.

159. *Privacy Highlights*, *supra* note 24; *Your Privacy*, *supra* note 24.

160. *Privacy Highlights*, *supra* note 24; *Your Privacy*, *supra* note 24; supra text accompanying note 151.

161. *See supra* text accompanying note 152.

162. *Your Privacy*, *supra* note 24; *see also supra* Part V.

163. Or assuming genetic information held by DTC genetic testing companies is constitutionally protected through the extension of the reasoning in *Carpenter*, Fourth Amendment protections may apply.

164. *See supra* text accompanying notes 140–44.

Under the third-party consent doctrine, the third party must have authority to give consent.[165] While the Supreme Court has not ruled on the application of third-party consent in relation to the closed container doctrine, multiple circuit courts have established rules on the issue.[166] In *United States v. Block*, the Fourth Circuit ruled a mother could not provide consent for a search of her child's footlocker located in his room if it was for his exclusive use.[167] Similarly, the Third Circuit ruled "a third party lacks authority to consent to a search of an area in which the target of the search has not 'relinquished his privacy.'"[168] Explaining the decision, the Third Circuit stated that *Randolph*[169] does not apply to personal effects and a computer is a personal effect.[170]

The Tenth Circuit even created a four-factor test to determine whether a third party has authority to consent to a search of a closed container.[171] The first factor is whether the container is one that has historically commanded a high degree of privacy.[172] To help the first factor analysis, common life experiences are used to determine a reasonable expectation of privacy.[173] Common life experiences may include the general belief that "enclosed spaces" have high privacy expectations and are at their highest expectation of privacy when briefly under control of another.[174]

The second factor in the Tenth Circuit test is precautions taken by the owner demonstrating their subjective expectation of privacy, such as locking or forbidding anybody from opening the container.[175] The third

165. United States v. Matlock, 415 U.S. 164, 164, 171 (1974); United States v. Block, 590 F.2d 535, 539–40 (4th Cir. 1978). This concept also touches on traditional property principles of joint ownership. When individuals have joint ownership of property, both have an interest in the property and one joint owner cannot transfer the property interest of the other joint owner. Cacchio, *supra* note 6, at 232. DNA submitted to DTC genetic testing companies poses a new issue. Family members have property interests in their DNA, but now these companies are contractually claiming that by submission, the company owns that genetic information. Cacchio, *supra* note 6, at 232.

166. *See, e.g.*, United States v. King, 604 F.3d 125, 137 (3d Cir. 2010); United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1991); United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978).

167. 590 F.2d at 541–42.

168. United States v. Stabile, 633 F.3d 219, 232 (3d Cir. 2011) (quoting *King*, 604 F.3d at 137).

169. Georgia v. Randolph, 547 U.S. 103, 106 (2006) (ruling a present co-tenant who refuses a consent search trumps the consenting co-tenant).

170. *King*, 604 F.3d at 137; *Stabile*, 633 F.3d at 233.

171. *Salinas-Cano*, 959 F.2d at 864.

172. *Id.*

173. *Id.*

174. *Id.* (quoting United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978)).

175. *Id.*

factor asks whether the search was initiated at the request of the third party for safety reasons and weighs against protection.[176] The fourth and final factor is whether the third party expressed his lack of interest in the object to the official conducting the search.[177]

The closed container doctrine and third-party consent are both applicable to genetic information. Generally, if Person A has no authority to give consent, then Person A cannot give consent for Person B.[178] In *Block*, a mother could not consent to a search of her child's footlocker.[179] The child in *Block* is like Person B[180] because the inherent privacy of DNA suggests exclusive use.[181]

Application of the Tenth Circuit test to genetic information suggests that Person A[182] does not have authority to consent to the use of Person B's[183] genetic information.[184] The first factor weighs heavily in favor of the inability to grant consent. Considering common life experiences for privacy expectations of genetic information, genetic information reasonably enjoys the highest expectation of privacy like enclosed spaces.[185] Steps taken by DTC genetic testing companies to maintain privacy, the passage of GINA, and the sensitive treatment by the Court all signal a high expectation of privacy in genetic data.[186]

According to the rationale of the Tenth Circuit, privacy expectations are greatest when an object is under control of another.[187] This rationale supports application of the Tenth Circuit test to genetic information. When DNA and corresponding information is submitted to DTC genetic testing companies, privacy expectations would be at the highest peak

176. *Id.* This factor is particularly strong in domestic violence cases where the third party consents to a search. *See* United States v. Waller, 426 F.3d 838, 848 (6th Cir. 2005) (citing *Salinas-Cano*, 959 F.2d at 864) ("[O]fficers invited to search an item during a response to a domestic violence report.").

177. United States v. Robinson, 999 F. Supp. 155, 162 (D. Mass. 1998) (citing *Salinas-Cano*, 959 F.2d at 864–65).

178. *See* United States v. Matlock, 415 U.S. 164, 171 (1978); United States v. Block, 590 F.2d 535, 540 (4th Cir. 1978). In the case of genetic information, Person A is the individual submitting the DNA to the genetic testing company. Person B is the familial match who was discovered only because of Person A's submission.

179. 590 F.2d at 542.

180. *See supra* note 178 and accompanying text.

181. *See Block*, 590 F.2d at 542; Cacchio, *supra* note 6, at 223.

182. *See supra* note 178 and accompanying text.

183. *See supra* note 178 and accompanying text.

184. *See* United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1991).

185. *See supra* text accompanying notes 172–74.

186. *See supra* text accompanying notes 131–34.

187. *Salinas-Cano*, 959 F.2d at 864 (citing United States v. Block, 590 F.2d 535, 541 (4th Cir. 1978)).

when in the hands of the third-party company.[188] By applying *Carpenter's* rationale to extend privacy expectations to genetic information,[189] it would further support the inability of Person A[190] to give consent for Person B's[191] genetic information.

The precautions factor of the Tenth Circuit test also weighs heavily in favor of Person A's[192] inability to give consent for the use of Person B's[193] DNA. Assuming Person A and Person B have joint ownership over the DNA,[194] Person B likely illustrates his subjective expectation of privacy in his genetic information. Like locking a container or prohibiting others to access the container, many individuals take steps to keep their genetic information private. These steps can include password protection of internet accounts and shredding sensitive documents.[195] Subjective intent could also be inferred from Person B's[196] refusal to submit his genetic information to a DTC genetic testing company, or even the outright condemnation of Person A's[197] completion of the test.[198] There is one issue with this factor, however. Most of the time, Person B[199] is unaware of Person A's[200] DNA sample submission to a genetic testing company.[201]

The third factor, whether the consent search was for safety purposes of the household, weighs in favor of Person A's[202] inability to grant consent for a search of a closed container.[203] Unlike domestic violence cases where this factor weighs extremely in favor of another to give consent, that concern is not present in submission of genetic information for genetic testing purposes.[204] When Person A[205] submits a DNA sample

188. *See id.*
189. *See supra* Part V.
190. *See supra* note 178 and accompanying text.
191. *See supra* note 178 and accompanying text.
192. *See supra* note 178 and accompanying text.
193. *See supra* note 178 and accompanying text.
194. *See supra* note 165 and accompanying text.
195. *See supra* text accompanying note 151.
196. *See supra* note 178 and accompanying text.
197. *See supra* note 178 and accompanying text.
198. *See* United States v. Salinas-Cano, 959 F.2d 861, 864 (10th Cir. 1991)
199. *See supra* note 178 and accompanying text.
200. *See supra* note 178 and accompanying text.
201. Due to the ability of DTC genetic testing companies to match family members to the level of third cousin, Person A could be a distant cousin of Person B, making it very unlikely that Person B will ever find out about Person A's submission.
202. *See supra* note 178 and accompanying text.
203. *See Salinas-Cano*, 959 F.2d at 864; *see also supra* text accompanying note 176.
204. *See Salinas-Cano*, 959 F.2d at 864; *see supra* text accompanying note 176.
205. *See supra* note 178 and accompanying text.

to a genetic testing company, the purpose is for hereditary medical conditions, heritage, and the possibility to connect with distant family members.[206]

Finally, verbalizing the lack of interest to the official conducting the search supports the inability for Person A[207] to consent.[208] When law enforcement locates Person B[209] from Person A's[210] DNA submission, Person B[211] has no way of knowing the search occurred because no warrant was produced.[212] It also seems unlikely that Person A[213] will make every other possible Person B[214] (familial match) aware that he submitted his DNA for testing. This would make it nearly impossible for potential Person B's[215] (familial matches) to be made aware of the risk and the implications of this information being shared.

VII. CONCLUSION

Even though genetic information is inherently sensitive and immutable, it enjoys very little legal protection.[216] From its inception, the intent of the Fourth Amendment was to protect against unnecessary, overly broad searches that arose from a general warrant during colonial times.[217] When law enforcement utilizes long-range familial matches, law enforcement is essentially executing a general warrant; the government rummaging around in inherently personal and private information, looking for probable cause to obtain a warrant.[218]

As these databases continue to grow, privacy concerns will continue to flourish.[219] In order to protect against law enforcement's warrantless intrusions, the Fourth Amendment can provide protection for genetic information. By extending Fourth Amendment privacy protections to

206. *See* Edward C. Baig, *Ancestry Launches DNA Health Service that Will Compete with 23andMe*, USA TODAY (Oct. 15, 2019), https://www.usatoday.com/story/tech/2019/10/15/ancestry-launches-dna-health-tests-assess-your-genetic-risks/3977076002/.

207. *See supra* note 178 and accompanying text.

208. *See Salinas-Cano*, 959 F.2d at 864; *supra* text accompanying note 177.

209. *See supra* note 178 and accompanying text.

210. *See supra* note 178 and accompanying text.

211. *See supra* note 178 and accompanying text.

212. *See supra* text accompanying note 13. This inability to know the search occurred is especially true when law enforcement used the public database GEDMatch.

213. *See supra* note 178 and accompanying text.

214. *See supra* note 178 and accompanying text.

215. *See supra* note 178 and accompanying text.

216. *See* Chen, *supra* note 6; *supra* note 15 and accompanying text.

217. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971).

218. *See* Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018).

219. *See supra* Part I.

genetic information through *Carpenter*, the third-party consent doctrine, and closed container doctrine, the Supreme Court would safeguard the protections the Framers intended to enshrine in the Fourth Amendment.