"23 AND PLEA": LIMITING POLICE USE OF GENEALOGY SITES AFTER *CARPENTER V. UNITED STATES*

Antony Barone Kolenc ∗

∗ Antony Barone Kolenc (J.D., University of Florida College of Law) has been a professor at University of North Texas Dallas College of Law and Florida Coastal School of Law. He served as a Lieutenant Colonel in the Air Force Judge Advocate General's Corps before retiring in 2012. He would like to thank U.S. Magistrate Judge Patricia D. Barksdale for her assistance in developing the idea for this paper.

I. INTRODUCTION[1]

The police pulled up to the Oregon nursing home with a search warrant signed by a county judge. Their suspect: a bed-ridden, 73-year-old man who also might be the elusive Golden State Killer who murdered 13 women and raped dozens more in the 1970s and 1980s. Without getting a warrant, law enforcement officers had narrowed their search for the killer using a public genealogy website with DNA[2] test results uploaded by hundreds of thousands of people. Their final clue had been that this suspect—along with the Killer—had a genetic mutation

---

[1] This introduction is drawn from *DNA Used in Hunt for Golden State Killer Previously Led to Wrong Man*, NBC NEWS (Apr. 28, 2018, 3:45 PM), https://www.nbcnews.com/news/us-news/dna-used-hunt-golden-state-killer-previously-led-wrong-man-n869796; and Benjamin Oreskes, et al., *False Starts in Search for Golden State Killer Reveal the Pitfalls of DNA Testing*, L.A. TIMES (May 4, 2018), https://www.latimes.com/local/lanow/la-me-ln-golden-state-killer-dna-20180504-story.html.

[2] "DNA, or deoxyribonucleic acid, is the genetic material found in the nucleus of cells, and is often referred to as the 'blueprint of life.' . . . The bases or components of DNA are four chemicals: Cytosine, Guanine, Thymine, Adenine." Jules Epstein, *"Genetic Surveillance"—The Bogeyman Response to Familial DNA Investigations*, 2009 U. ILL. J.L. TECH. & POL'Y 141, 143 (2009).

possessed by less than 3% of Caucasians in the genealogy database. Without asking the man's permission as he lay in bed, the police swabbed a DNA sample from his mouth and sent it for lab testing, comparing it to the DNA of the Golden State Killer found at a crime scene decades earlier. The result: no match; the man was innocent. The police tested a second suspect—also no match. Finally, on the third try, they got their man: Joseph De Angelo, an ex-cop now facing rape and murder charges and whose DNA matched the real killer.

This story of mistaken identity, breath-taking DNA testing technology, and hard-boiled police work has become the first chapter in a series of increasingly common criminal investigations that rely on genetic samples tested by genealogy companies such as 23andMe and Ancestry, two of the most popular services, and loaded on public websites such as Ysearch or GEDmatch, the site that led police to the Golden State Killer.[3] Law enforcement officers all over the United States are now using similar tactics in hundreds of cases to catch alleged killers and have logged their first jury verdict conviction in one such case in 2019.[4] While some commercial genealogy sites, like Ancestry and 23andMe, have a policy that requires a warrant from the police before disclosing genetic data, sites like GEDmatch have less stringent policies.

But some privacy advocates believe warrantless searches of DNA databases could violate the Fourth Amendment and other privacy interests and lead to police abuses. They suggest the U.S. Supreme Court's 2018 decision, *Carpenter v. United States*,[5] provides a constitutional basis for ending these law enforcement tactics.[6]

---

[3] Companies such as Parabon NanoLabs now work with police and GEDmatch to load DNA from hundreds of cases. *See* Sarah Zhang, *How a Tiny Website Became the Police's Go-To Genealogy Database*, ATLANTIC (June 1, 2018), https://www.theatlantic.com/science/archive/2018/06/gedmatch-police-genealogy-database/561695/.

[4] Hundreds of cases are now investigated using DNA evidence. *See* Heather Murphy, *How Your DNA Could Solve a Murder*, WEEK (June 27, 2018), https://theweek.com/articles/841864/how-dna-could-solve-murder. In June 2019, a jury convicted William Talbott II of two 1987 murders based on DNA evidence—the first verdict in such a case. *See* Robert Gearty, *Washington Cold Case Solved Using DNA and Genetic Genealogy Results in Landmark Verdict*, FOX NEWS (June 29, 2019), https://www.foxnews.com/us/cold-case-solved-dna-genetic-genealogy-landmark-verdict.

[5] 138 S. Ct. 2206, 2222 (2018).

[6] *See* Ken Strutin, *DNA Without Warrant: Decoding Privacy, Probable Cause and Personhood*, 18 RICH. J.L. & PUB. INT. 319, 364 (2015) ("[W]hen technology advances to efficiently collect and catalog shed DNA, biological tracking data, another kind of privacy interest might be recognized."); *see also* Rebecca Lund, *It Is All in the Family: Using Online DNA Profiles to Identify Suspects*, VAND. J. ENT. & TECH. L. (Oct. 21, 2018), http://www.jetlaw.org/2018/10/21/it-is-all-in-the-family-using-online-dna-profiles-to-identify-suspects/ ("Should police be permitted to create fake profiles and upload [DNA] data without prior authorization? In the wake of [*Carpenter*] . . . many are left wondering whether this will continue to be permitted.").

Part II of this Article briefly examines the *Carpenter* decision and the privacy interests implicated by DNA testing and private genealogy websites. Part III discusses whether, after *Carpenter*, police searches of genealogy websites trigger Fourth Amendment protection. Part IV explores the third-party doctrine, assessing its post-*Carpenter* viability in the DNA context. Concluding the Fourth Amendment provides limited protection, Part V seeks alternative solutions to the noted privacy concerns.

II. *CARPENTER*, THE FOURTH AMENDMENT, AND DNA TESTING

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[7] In the context of DNA testing, the term "persons" includes bodily fluids and DNA.[8] When analyzing a search issue, courts first ask whether the item searched by police (e.g., a DNA test in a private database) is protected by the Fourth Amendment.[9] If so, courts then determine whether the search was reasonable.[10] The Supreme Court's "basic rule" is that "'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.'"[11]

This Article explores the issue of warrantless police searches of private genealogy databases after *Carpenter*, focusing on whether the Fourth Amendment protects DNA test results—both a person's own results and those of their biological relatives—and whether the "third-party doctrine"[12] is viable in that context. If the Fourth Amendment applies, this Article assumes without discussion that any warrantless search would be *per se* unreasonable (i.e., a constitutional violation).

This part of the Article briefly recounts basic Fourth Amendment principles: the historical property-based approach, the modern method based on "reasonable expectations of privacy," and the development of the third-party doctrine. Next, it examines the *Carpenter* decision and its potential impact on

---

7 U.S. CONST. amend. IV.

8 Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 808–09 (2016).

9 *See* Katz v. United States, 389 U.S. 347, 351–52 (1967).

10 *See id.*

11 Arizona v. Gant, 556 U.S. 332, 338 (2009) (quoting *Katz*, 389 U.S. at 357).

12 The third-party doctrine essentially holds that, "when a person voluntarily gives information to a third party, even for a limited, specific purpose, and that third party delivers the information to law enforcement, the government's acquisition of the information cannot be defined as a search." Laurie Buchan Serafino, *"I Know My Rights, So You Go'n Need a Warrant for That": The Fourth Amendment,* Riley*'s Impact, and Warrantless Searches of Third-Party Clouds*, 19 BERKELEY J. CRIM. L. 154, 166 (2014).

Fourth Amendment law. Finally, it explores privacy interests associated with DNA testing and the storage of test results in both government-controlled and private genealogy databases and websites.

A. Historical Fourth Amendment Analysis and the Carpenter *Decision*

In *Carpenter v. United States*, the Supreme Court found that the police conducted a search under the Fourth Amendment when they accessed third-party, historical records of a suspect's cell-phone location.[13] In its decision, the Court deepened privacy protections for cell-phone usage and refused to apply the third-party doctrine to negate those protections. It recounted the two "guideposts" of the Fourth Amendment: (1) securing "the privacies of life" against "arbitrary power," and (2) placing "obstacles in the way of a too permeating police surveillance."[14]

Privacy advocates would like to conscript these guideposts into service to protect information on genealogy sites from the police. Seeing *Carpenter* as a "landmark ruling on how to apply the Fourth Amendment's protections in the digital world," they envision its application to genealogy databases, which "contain a wealth of deeply personal information about one's ancestry and medical conditions."[15] They contend the current "division between privacy in information technology and in information biologics does not further the ends of justice" and they ask why the cell phone should receive more constitutional protections than the contents of the human body.[16]

1. The Dual Track of the Fourth Amendment

The trajectory of Fourth Amendment jurisprudence has followed two tracks. Traditionally, it had been "tied to common-law trespass" and focused on whether the Government "obtains information by physically intruding on a constitutionally protected area."[17] This common-law property sentiment was best represented by *Entick v. Carrington*,[18] a well-known English case in which Lord Camden stated that the law "holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he

---

13 Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

14 *Id.* at 2214 (citations omitted).

15 Matt Ford, *How the Supreme Court Could Rewrite the Rules for DNA Searches*, NEW REPUBLIC (Apr. 30, 2018), https://newrepublic.com/article/148170/supreme-court-rewrite-rules-dna-searches.

16 Strutin, *supra* note 6, at 366.

17 *Carpenter*, 138 S. Ct. at 2213 (citations omitted) (discussing Fourth Amendment precedents).

18 Entick v. Carrington (1765) 95 Eng. Rep. 807 (KB).

is a trespasser, though he does no damage."[19] For over a century, the Court relied on this property-based approach when interpreting the Fourth Amendment, finding a search occurs when police trespass on a property interest. It followed this first track in earlier cases, such as *Olmstead v. United States*,[20] and again very recently in *Florida v. Jardines*[21] and *United States v. Jones*,[22] where the Court emphasized the continued viability of the property-based approach today.

Then, in the 1960s, the Supreme Court "recognized that 'property rights are not the sole measure of Fourth Amendment violations.'"[23] The landmark case of *Katz v. United States*[24] created a second track, finding that the Fourth Amendment "'protects people, not places,' and expanded [the] conception of the Amendment to protect certain expectations of privacy as well."[25] Today, not all Justices agree the *Katz* test is valid,[26] and some have complained that it leads to inconsistent and nonsensical results.[27] But, as *Carpenter* explained, *Katz* held that "[w]hen an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause."[28]

---

19 *Id.* at 817.

20 277 U.S. 438, 464 (1928) (finding no Fourth Amendment search when government agents tapped phone wires on the public streets due to a lack of trespass in "the houses or offices of the defendants"); *see also* Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28 ALB. L.J. SCI. & TECH. 73, 79 (2018) (discussing *Olmstead*).

21 569 U.S. 1, 11 (2013) (finding a Fourth Amendment search when police trespassed with drug-sniffing dogs on curtilage of home)*; see also* Ormerod & Trautman, *supra* note 20, at 79 (discussing *Jardines*).

22 565 U.S. 400, 404 (2012) (finding a Fourth Amendment search when police trespassed on a private vehicle to place a GPS tracker); *see also* Ormerod & Trautman, *supra* note 20, at 79 (discussing *Jones*).

23 *Carpenter*, 138 S. Ct. at 2213 (discussing modern Fourth Amendment cases).

24 389 U.S. 347, 353 (1967) (finding a Fourth Amendment search when agents placed a listening device on a public telephone booth due to Katz's "reasonable expectation of privacy").

25 *Carpenter*, 138 S. Ct. at 2213.

26 *Id.* at 2239 (Thomas, J., dissenting) (arguing *Katz* "strays" far from the constitutional text "by focusing on the concept of 'privacy,'" which is nowhere in the Constitution, and contending the Founders understood "liberty and privacy rights" "in terms of property rights").

27 *Id.* at 2263 (Gorsuch, J., dissenting). Justice Gorsuch derided results like *Florida v. Riley*, 488 U.S. 445 (1989), which says a "police helicopter hovering 400 feet above a person's property invades no reasonable expectation of privacy. Try that one out on your neighbors." *Carpenter*, 138 S. Ct. at 2266. Just Gorsuch also questioned *California v. Greenwood*, 486 U.S. 35 (1988), which holds that a "person has no reasonable expectation of privacy in the garbage he puts out for collection," and he expressed doubt "that most people spotting a neighbor rummaging through their garbage would think they lacked reasonable grounds to confront the rummager." *Carpenter*, 138 S. Ct. at 2266.

28 *Carpenter*, 138 S. Ct. at 2213 (majority opinion).

The new *Katz* analysis grew over time, but not without difficulties. This led the Supreme Court to develop the third-party doctrine in *United States v. Miller*[29] and *Smith v. Maryland*[30] to explain why a Fourth Amendment search under *Katz* does not occur when a suspect entrusts private information to a third party, who then betrays the suspect to the police.[31] With its origin in cases involving confidential informants, the doctrine espouses the general rule that "if information is possessed or known by third parties, then, for purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information."[32]

As the new millennium dawned, the Supreme Court began to recognize that quickly evolving advances in technology might require a sea change in its dual-track Fourth Amendment jurisprudence. In 2001, Justice Antonin Scalia charted an initial course to deal with emerging technologies in *Kyllo v. United States.*[33] As the *Carpenter* Court explained, *Kyllo* rejected a "mechanical interpretation" of the Fourth Amendment in holding that a thermal imager could not be used by police to detect heat radiating from a suspect's home.[34] "Because any other conclusion would leave homeowners 'at the mercy of advancing technology,' [the Court] determined that the Government—absent a warrant—could not capitalize on such new sense-enhancing technology to explore what was happening within the home."[35]

A decade later, Justice Sonia Sotomayor argued in *Jones* that the digital age made it necessary to revisit "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" because "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[36] She contended the Fourth Amendment should not "treat secrecy as a prerequisite for privacy."[37]

Two years later, in *Riley v. California*,[38] Chief Justice John Roberts delivered the first of two blockbuster cell-phone decisions. Recognizing the

---

29 425 U.S. 435, 443 (1976).

30 442 U.S. 735, 743–44 (1979).

31 *See id.* (finding no Fourth Amendment search when police used a pen register because Smith assumed the risk when he conveyed dialed numbers to the third-party phone company); *Miller*, 425 U.S. at 443 (establishing the "third-party doctrine" and finding no Fourth Amendment search when police subpoenaed Miller's banks records, including months of canceled checks).

32 Ormerod & Trautman, *supra* note 20, at 111.

33 533 U.S. 27, 34 (2001) (finding a Fourth Amendment search where police used a thermal imaging device to intrude on the private areas of a home).

34 Carpenter v. United States, 138 S. Ct. 2206, 2214.

35 *Id.*

36 United States v. Jones, 565 U.S. 400, 417 (Sotomayor, J., concurring).

37 *Id.* at 418.

38 573 U.S. 373 (2014) (finding a Fourth Amendment search when police automatically conducted a search of the contents of an arrestee's cell phone).

"immense storage" of sensitive information on cell phones, the *Riley* Court unanimously ruled that law enforcement must obtain a Fourth Amendment warrant to obtain a cell phone's contents as part of a search incident to a lawful arrest.[39] Then, four years later, Chief Justice Roberts gave an even more decisive, though more controversial, ruling on the matter of cell-phone privacy in *Carpenter*.

2. The *Carpenter* Decision and Its Potential Impact on Police Action

In *Carpenter*, Chief Justice Roberts (joined by the Court's four "liberal" members) expanded privacy rights and held that law enforcement conducts a search under the Fourth Amendment when it accesses historical cell-site location information ("CSLI"), which provides a "comprehensive chronicle of the user's past movements."[40] Significantly, the Court re-interpreted its traditional understanding of a person's privacy in their physical movements in light of advances in technology.

Timothy Carpenter and his accomplices (along with their cell phones) robbed nine retail stores in Michigan and Ohio over a four-month period.[41] Using court orders under the Stored Communications Act ("SCA")[42]—which does not require probable cause under the Fourth Amendment—the Federal Bureau of Investigation ("FBI") obtained business records from two wireless commercial carriers, disclosing CSLI for Carpenter's phone.[43] Using this data (over 12,000 cell location points), the FBI retraced Carpenter's movements over those four months, corroborating other evidence and placing him near the scenes of the charged robberies.[44]

In holding the FBI conducted a Fourth Amendment search, the Court observed that the collection of third-party CSLI data intersected two lines of cases: (1) that stemming from *United States v. Knotts*[45] and *United States v.*

---

39 *Carpenter*, 138 S. Ct. at 2214 (citations omitted) (discussing *Riley*).

40 Cell-site location information ("CSLI") is continuously gathered as a cell phone automatically connects to a cell-site radio antenna and "generates a time-stamped record." *Id.* at 2211.

41 *Id.* at 2212.

42 The SCA requires only that police provide a court with "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." 18 U.S.C.A. § 2703(d) (West 2019).

43 *Carpenter*, 138 S. Ct. at 2212.

44 *Id.* at 2212–13. Interestingly, *Carpenter* based its ruling on the "more sophisticated systems . . . already in use or in development" in 2018, rather than limiting its view to the technological facts of the case in 2011. *Id.* at 2218–19 (citations omitted).

45 460 U.S. 276, 281 (1983). *Carpenter* explained that *Knotts* approved police use of a beeper planted in a container (prior to purchase by Knotts) that "augmented" police visual surveillance (by ground and air) "to aid in tracking a vehicle through traffic" from Minneapolis "to Knotts's cabin in Wisconsin, relying on the beeper's signal to help keep the vehicle in view." *Carpenter*,

Jones,[46] which address "a person's expectation of privacy in his physical location and movements," and (2) that stemming from the third-party doctrine created in *United States v. Miller*[47] and *Smith v. Maryland*.[48] The Court concluded the warrantless police request for Carpenter's CSLI violated his "reasonable expectation of privacy in the whole of his physical movements."[49]

Chief Justice Roberts explained that CSLI allows for "near perfect surveillance" (like an "ankle monitor") and that cell phones track their owners' movements "nearly exactly" because people "compulsively carry cell phones with them all the time . . . into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[50] Further, the "retrospective quality" of CSLI allows police to "travel back in time" for five years (the current data-retention policy of wireless carriers) and analyze data about a person who was not previously a suspect, retracing his whereabouts "every moment of every day."[51] For reasons discussed later, the Court also found the third-party doctrine should not be extended to this new technological area.[52]

The *Carpenter* Court's willingness to expand modern privacy rights while limiting the third-party doctrine has far-reaching implications. It is fair to consider whether the Court would take a similar approach in requiring the police to obtain a Fourth Amendment warrant before accessing DNA data on genealogy

---

138 S. Ct. at 2215. This was not a Fourth Amendment search "because '[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,'" and "the movements of the vehicle and its final destination had been 'voluntarily conveyed to anyone who wanted to look.'" *Id.* (citations omitted). The Court noted that *Knotts* had "reserved the question whether 'different constitutional principles may be applicable' if 'twenty-four hour surveillance of any citizen of this country [were] possible.'" *Id.* at 2215 (quoting *Knotts*, 460 U.S. at 284).

46 565 U.S. 400, 404–05 (2012). *Carpenter* explained that *Jones* invalidated a search by FBI agents who "installed a GPS tracking device on Jones's vehicle and remotely monitored the vehicle's movements for 28 days" because the police had physically trespassed on the vehicle to place the tracker. *Carpenter*, 138 S. Ct. at 2215. Five Justices had also "agreed that related privacy concerns would be raised by, for example, 'surreptitiously activating a stolen vehicle detection system' in Jones's car to track Jones himself, or conducting GPS tracking of his cell phone" because this type of monitoring "tracks 'every movement' a person makes" and "that 'longer term GPS monitoring . . . impinges on expectations of privacy'—regardless whether those movements were disclosed to the public at large." *Id.* at 2215 (quoting *Jones*, 565 U.S. at 415, 426, 428 (concurring opinions of Alito & Sotomayor, JJ., respectively)).

47 425 U.S. 435 (1976).

48 *Carpenter*, 138 S. Ct. at 2215–16 (explaining United States v. Miller, 425 U.S. 435 (1976) (no search of third-party bank records) and Smith v. Maryland, 442 U.S. 735 (1979) (no search of third-party phone numbers)).

49 *Id.* at 2219.

50 *Id.* at 2218.

51 *Id.*

52 The *Carpenter* Court's analysis of the third-party doctrine will be discussed below. *See infra* Part IV.

web sites.[53] Taking into account the two "guideposts" of the Fourth Amendment, one could argue the Constitution should secure "the privacies of life" contained in one's DNA from arbitrary police searches and place "obstacles" in the way of these searches that could permeate too far into an individual's heritage and health data.[54] Even Justice Neil Gorsuch, in dissent in *Carpenter*, recognized the concern in DNA cases: "Can the government . . . secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of *Katz*. But that result strikes most lawyers and judges today—me included—as pretty unlikely."[55]

Just as *Carpenter* reinterpreted the idea of privacy in physical movements, advocates hope the Supreme Court will broaden its understanding of privacy interests involving DNA. And just as *Carpenter* was willing to limit the third-party doctrine as applied to cell-phone technology, they hope the Court will similarly limit that doctrine based on advances in DNA testing and the ubiquity of "voluntary" genealogy tests in modern society. As one scholar argues, DNA is "the 'object' or container in which privacy inheres, not merely the data or contents," and both computers and "nuclear DNA contain more information than will be found in the home or ever could be. Thus, if the expectations of millions can define the privacy interest in cell phones, certainly the expectations of billions should decide the level of privacy in the human genome."[56]

B. Understanding Genetic Privacy and Genealogy Databases

Before applying a post-*Carpenter* Fourth Amendment analysis to DNA testing and genealogy websites, it is necessary to consider the biological processes at work and the spectrum of DNA-related privacy interests being claimed. This section provides basic information about DNA testing and proposes a model to form a common frame of reference when discussing the level of privacy associated with DNA test results.

1. The Promise of DNA and Its Analysis

As living organisms, human beings possess a complete set of genetic material—a genome—that dictates how they will grow, develop, and reproduce. Within the nucleus of each of the trillions of cells within human beings is a molecule of genetic material known as DNA, or deoxyribonucleic acid. It is inherited equally from a person's mother and father, carries critical genetic information, and is packaged in "divided bunches" on 23 paired, "thread-like

---

53 *See* Ford, *supra* note 15.

54 *Carpenter*, 138 S. Ct. at 2213–14 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

55 *Id.* at 2262 (Gorsuch, J., dissenting).

56 Strutin, *supra* note 6, at 363.

structures called chromosomes."[57] These paired chromosomes (one from mom and one from dad) contain two copies of each "gene," which is a segment of DNA containing "coding sequences that determine what the gene does (e.g., trigger premature gray hair), and non-coding sequences that determine when the gene is expressed (e.g., at age 20)."[58] Variants of each gene, known as "alleles," "occupy fixed positions (called a locus for one, loci for two or more) on a specific chromosome."[59] The allele holds the key to DNA identification analysis.

During the last century, as scientists worked to "sequence" the human genome, they discovered that the "vast majority of DNA—over 99.7 percent—is identical between two people."[60] But allele variations along the DNA strand, especially on 13 specific loci, allow scientists to "obtain [26] discrete measurements that help individuate one person from another."[61] These loci, in regions of DNA with no known coding function—"junk DNA"[62]—are now at the core of forensic DNA analysis.

Forensic DNA analysis "identifies the alleles at each of the 13 loci, determines the frequency with which the combination at a single locus occurs across the population, and then calculates a 'random-match probability,'" which is defined as "the probability that a person other than the suspect, randomly selected from the population, will have this profile."[63] Allele analysis not only helps identify specific individuals, but also a person's biological relatives. "Because these [26] alleles are directly inherited from one's biological parents, there is a significant probability that two people who share biological ties will also share a large number of alleles in common."[64]

The "advent of DNA technology" and forensic DNA testing based on allele analysis has been hailed by the Supreme Court as one of the "most significant scientific advancements of our era."[65] The Court has acknowledged the "undisputed utility" of DNA testing in the criminal justice system, noting its "unparalleled ability" to exonerate the wrongly convicted and "identify the guilty. It has the potential to significantly improve both the criminal justice

---

57 Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 294–95 (2010); Genetics Home Reference, *What Is a Chromosome?*, NAT'L INST. HEALTH (Aug. 20, 2019), https://ghr.nlm.nih.gov/primer/basics/chromosome.

58 Jessica D. Gabel, *Probable Cause from Probable Bonds: A Genetic Tattle Tale Based on Familial DNA*, 21 HASTINGS WOMEN'S L.J. 3, 7–8 (2010).

59 *Id.* at 8.

60 Murphy, *supra* note 57, at 294–95.

61 *Id.*

62 Gabel, *supra* note 58, at 8–9; *see also* Maryland v. King, 569 U.S. 435, 445 (2013) (discussing "junk DNA").

63 Epstein, *supra* note 2, at 143–44.

64 Murphy, *supra* note 57, at 295.

65 *King*, 569 U.S. at 442.

system and police investigative practices."[66] And its uses go beyond criminal justice. More recently, this same impetus has driven a lucrative private, commercial genealogy market for individuals seeking to learn more about their own heritage and to connect with biological relatives around the world.[67]

2. CODIS, NDIS, and Government-Run DNA Databases

A key part of the success of forensic DNA testing has been the development of a government-run database used to identify perpetrators of serious criminal acts. That effort began in earnest in 1990 with the creation of the Combined DNA Index System ("CODIS")—software developed by the FBI to help navigate DNA databases at state and local crime labs.[68] In 1994, Congress sanctioned CODIS with the DNA Identification Act, which also authorized the FBI to create a National DNA Index System ("NDIS"), a national database that also links with state and local crime labs.[69] CODIS helps law enforcement test unknown DNA samples gathered from crime scenes against DNA results gathered from known criminals.[70] As Justice Scalia explained, "[T]he CODIS system works by checking to see whether any of the [DNA] samples in the Unsolved Crimes Collection match any of the samples in the Convict and Arrestee Collection."[71]

CODIS has become "one of the largest genetic surveillance tools in the world," with "DNA profiles from over 14.3 million known individuals and from over 625,000 crime scene samples," and "has survived every legal challenge."[72] The number of samples collected has grown in the wake of the U.S. Supreme Court's 2013 decision approving state laws that allow for the collection of DNA from certain arrestees.[73] Now, over half of the states allow for DNA "test-on-arrest" with "varying standards and procedures in terms of qualifying

---

66 *Id.*

67 *See infra* Section II.B.3.

68 Gabel, *supra* note 58, at 13–14; *see also* Thomas Hale-Kupiec, *Immortal Invasive Initiatives? The Need for a Genetic "Right to be Forgotten"*, 17 MINN. J.L. SCI. & TECH. 441 (2016) (discussing the history of CODIS).

69 Gabel, *supra* note 58, at 14.

70 According to the U.S. Supreme Court, "CODIS sets uniform national standards for DNA matching and then facilitates connections between local law enforcement agencies who can share more specific information about matched STR profiles." *King*, 569 U.S. at 445. The Court expressed its understanding that "the information in the database is only useful for human identity testing" and that DNA "information is recorded only as a 'string of numbers.'" *Id*.

71 *Id.* at 473 (Scalia, J., dissenting).

72 Jason Kreag, *Going Local: The Fragmentation of Genetic Surveillance*, 95 B.U. L. REV. 1491, 1494 (2015).

73 *See King*, 569 U.S. at 465–66. That decision will be discussed below in Part III; *see also* Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 MINN. L. REV. 541, 551 (2016) ("DNA collection is now an accepted part of being arrested.").

offenses, timing for taking a sample, conditions for destroying samples, and their use in court proceedings."[74] This growing database not only makes it easier to find exact matches, but it also assists with "familial searching" for a relative of a criminal perpetrator.[75] Studies have shown that, if "the search threshold is set widely enough, it is 80 to 90 percent likely that a partial match search will include the relative in its results."[76]

CODIS is governed by strict standards and does not formally interface with databases that record criminal histories.[77] Thus, some law enforcement agencies continue to create local DNA databases that provide more search flexibility with less regulation.[78] These local databases often contain more private information than found in CODIS and are sometimes funded by for-profit enterprises.[79]

3. Private DNA Databases and Genealogy Websites

While CODIS and NDIS fought off legal attacks and became more efficient means for police to locate perpetrators, the private sector commercialized DNA testing to cater to the booming genealogy industry. The availability of cheap, easy, online genealogy websites fed the natural human desire to get in touch with one's roots. With genealogy becoming "the second most popular hobby in the U.S. after gardening," websites dealing with genealogy became "the second most visited category of websites, after pornography.[80] It's a billion-dollar industry that has spawned profitable websites, television shows, scores of books and—with the advent of over-the-counter genetic test kits—a cottage industry in DNA ancestry testing."[81]

The most popular of these commercial genealogy DNA services are 23andMe and Ancestry. Already, those two companies alone have tested and databased well over ten million DNA samples, with the number of customers more than doubling in 2017.[82] Because these genealogy-related DNA services

---

74 Strutin, *supra* note 6, at 346.

75 Murphy, *supra* note 57, at 297–98.

76 *Id.* at 298.

77 *See* Hale-Kupiec, *supra* note 68, at 470–71.

78 Kreag, *supra* note 72, at 1494 n.14.

79 *Id.* at 1497 (explaining local databases "often include genetic profiles" and are easier to access because "local agencies are free to search these databases . . . unconstrained by" federal limits); *see also* Logan & Ferguson, *supra* note 73, at 551.

80 Gregory Rodriguez, *How Genealogy Became Almost as Popular as Porn*, TIME (May 30, 2014), https://time.com/133811/how-genealogy-became-almost-as-popular-as-porn/.

81 *Id.*

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

seek to reveal much more than mere identification, they work differently than CODIS. Ancestry explains that its "autosomal DNA test" is different than the Y-chromosome or mitochondrial DNA tests because it surveys "a person's entire genome at over 700,000 locations. It covers both the maternal and paternal sides of the family tree, so it covers all lineages."[83] And with customers wanting ever more information about their backgrounds and their bodies, the success of these genealogy projects has spawned spin-off companies, such as Habit and Promethease, which take the DNA files prepared by 23andMe and Ancestry and "provide a breakdown of people's diet or health risks, frequently with little oversight from regulators."[84]

One such spinoff service is GEDmatch, the website successfully used by law enforcement officers in the Golden State Killer case (and many other cases since).[85] GEDmatch allows users (at no cost) to upload their DNA test results (such as from Ancestry and 23andMe) to a centralized website.[86] From there, GEDmatch converts the original data "to a form that makes it more efficient for the software to perform searches and comparisons" and loads it into a relational database in a "compressed binary format" called "tokenization."[87] By using services such as GEDmatch, users can maximize their chances of finding new biological relatives by comparing their DNA results across a broader spectrum than the individual databases maintained separately by each commercial service.

The massive expansion of the genealogy industry has led to the curious situation where millions of average, law-abiding persons have voluntarily given their DNA to corporations (for a fee) to test and store in massive databases. And this practice has blossomed even while a privacy battle has been waging in the courts over government efforts through CODIS and NDIS to take DNA samples from those convicted and accused of crimes for the primary purpose of identification. Thus, it was only a matter of time before savvy law enforcement officers recognized the potential in these private DNA databases, filled with new and diverse samples, to locate criminal perpetrators (or their biological families) who had evaded discovery because their DNA samples had never been loaded into government-controlled databases.

---

[83] *AncestryDNA - Frequently Asked Questions*, ANCESTRY, https://www.ancestry.com/dna/en/legal/us/faq#about-3 (last visited Aug. 29, 2019).

[84] Regalado, *supra* note 82.

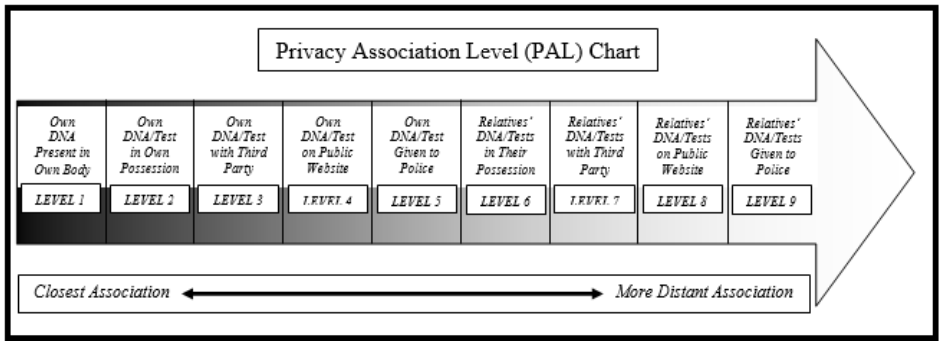
[85] *See* Avi Selk, *The Ingenious and 'Dystopian' DNA Technique Police Used to Hunt the 'Golden State Killer' Suspect*, WASH. POST (Apr. 28, 2018), https://www.washingtonpost.com/news/true-crime/wp/2018/04/27/golden-state-killer-dna-website-gedmatch-was-used-to-identify-joseph-deangelo-as-suspect-police-say/?noredirect=on.

[86] *GEDmatch.Com Terms of Service and Privacy Policy*, GEDMATCH (May 18, 2019), https://www.gedmatch.com/tos.htm.

[87] *Id.*

4. Charting Privacy Association Levels (PALs)

Before analyzing DNA privacy issues through the lens of the Fourth Amendment, it is helpful to have a common frame of reference. The chart below outlines what might be called "privacy association levels" ("PALs"), which are intended only in a descriptive and referential way. No doubt, there are other ways to conceptualize the spectrum of involved privacy interests, and some may disagree about the order of placement of these items on the spectrum. But the chart is intended merely to provide a common reference point for discussion for the remainder of this Article.



As the chart suggests, the privacy area of closest association to the subject of a criminal investigation is when the DNA is still present in the subject's body. The PAL chart moves progressively away from this closest privacy association when the subject voluntarily provides DNA test results to third parties, the public at large, and, finally, the police. The chart next moves to the privacy interest (if any) that criminal subjects have in the DNA of biological relatives, following a similar attenuation when those relatives provide their DNA results to third parties, the public at large, and, finally, the police. The discussions throughout this Article will reference these various scenarios by their PAL level (e.g., a Level 2 search of a criminal subject's DNA test results while still in the owner's personal possession).

III. APPLYING THE FOURTH AMENDMENT TO DNA TESTS AFTER *CARPENTER*

Part III of this Article examines whether the Fourth Amendment applies to police searches of DNA databases and private genealogy sites. It approaches the problem from the perspective of individual subjects of criminal investigation, first applying the modern analysis begun in *Katz* and asking whether criminal subjects possess a reasonable expectation of privacy in their own DNA and in the DNA of their biological relatives. The discussion next considers those same questions under the traditional property-based approach to the Fourth Amendment, which has made a comeback in recent years. This Article separately

addresses the third-party doctrine in Part IV. While third-party considerations could be examined as part of a *Katz* analysis, the discussion is clearer if analyzed separately, as the Court did in *Carpenter*.

A. Analyzing Genetic Privacy Under the Katz *Approach*

The "reasonable expectation of privacy" analysis created in *Katz* has become the lodestar of Fourth Amendment case law, even though the Supreme Court has recently labored to restore the traditional property-rights analysis to its rightful place in Fourth Amendment thinking. As Justice Clarence Thomas has explained, the Supreme Court developed this modern analysis by adopting the methodology proposed by Justice John Marshall Harlan in his concurring opinion in *Katz*, in which he "identified a 'twofold requirement' to determine when the protections of the Fourth Amendment apply: 'first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."'"[88] Over time, the Supreme Court has "minimized" its inquiry into subjective intent, leaving only the "objective prong—the 'reasonable expectation of privacy' test that the Court still applies today."[89]

Referencing the various PALs in the chart at the end of Part II, this section focuses on whether, under a *Katz* analysis, subjects of criminal investigations have a reasonable expectation of privacy in their own DNA and test results and in the DNA tests of their biological relatives.

1. Privacy at the Point of DNA Collection: Levels 1 and 2

As the descriptive PAL chart suggests above, the closest privacy association for DNA testing is while the DNA is still within the criminal subject's body, prior to collection by the police—a Level 1 association. Here, the Supreme Court and legal scholars agree the Fourth Amendment protects bodily fluids (and other biological items) while still attached to the criminal subject.[90] The Court has made this point explicit in the DNA context, stating it "can be agreed that using a buccal swab on the inner tissues of a person's cheek in order to obtain DNA samples is a search. Virtually any 'intrusio[n] into the human body,' will

---

88 Carpenter v. United States, 138 S. Ct. 2206, 2237 (2018) (Thomas, J., dissenting).

89 *Id.* at 2238.

90 As Professor Andrew Ferguson has noted, the Fourth Amendment's reference to "persons" has been interpreted by the courts to include "intrusions into the human body to draw blood or obtain saliva," as well as to "excretions from the human body, such as urine and breath in a breathalyzer." Ferguson, *supra* note 8, at 854–55. "DNA recovered from a person was obviously not considered by the Founders, but has been granted limited protection by the courts." *Id.* at 855.

work an invasion of 'cherished personal security' that is subject to constitutional scrutiny."[91]

Similarly, PAL Level 2 is primarily a theoretical construct that envisions the situation where a criminal subject has not turned over DNA (or results of a DNA test) to a third party, but where the DNA has left the subject's body. In this straightforward scenario, the DNA or test results should be treated as an "effect" of the subject, much like a wedding ring or wallet in one's pocket, and the police should be held to the same Fourth Amendment standards as any physical object in a person's possession, typically considered within a person's reasonable expectation of privacy.[92]

While it is undisputed that criminal subjects have a reasonable expectation of privacy in their bodies and items within their possession, two topics merit a pause for further consideration: (1) automatic DNA collection from arrestees, and (2) DNA that is "abandoned" by criminal subjects.

First, in *Maryland v. King*,[93] the Supreme Court approved Maryland's practice of automatically collecting DNA samples from certain arrestees.[94] It had already been assumed as an exception to the Fourth Amendment's warrant requirement that "the state does not need probable cause to compel DNA samples from convicted offenders [who] are deemed to have a reduced expectation of privacy in their genetic information."[95] In *King*, the Court went further, allowing police to collect DNA samples from certain arrestees during the booking process (and submitting that DNA to CODIS) as a means of "identifying" them—a theory derided by Justice Scalia in dissent.[96] Therefore, as long as the police possess a (theoretical) interest in identifying certain arrestees, the Supreme Court apparently will allow them to run DNA tests on samples collected without probable cause as an automatic part of the booking process.

Second, DNA that has been "abandoned" by criminal suspects by exiting their bodies—for instance, by spitting on the sidewalk, scratching skin cells from

---

91 Maryland v. King, 569 U.S. 435, 446 (2013) (citations omitted) (providing examples to include drawing blood, "scraping an arrestee's fingernails to obtain trace evidence," and breathalyzer tests).

92 *See, e.g.*, Minnesota v. Dickerson, 508 U.S. 366 (1993) (holding that the seizure of a lump of cocaine found in a suspect's pocket that was not immediately recognized as contraband by the officer is unconstitutional).

93 569 U.S. 435 (2013).

94 *See generally id.*

95 Gabel, *supra* note 58, at 33 (citing United States v. Kincade, 379 F.3d 813, 839 (9th Cir. 2004)).

96 In dissent, Justice Scalia contended Maryland did not use the arrestee's DNA for identification but for the purpose of solving unsolved crimes. *King*, 569 U.S. at 473 (Scalia, J., dissenting) (explaining the "logical" thing for Maryland to do if identification were its aim would be to compare the arrestee's DNA against CODIS's "Convict and Arrestee Collection" known database; however, Maryland was actually comparing the arrestee's samples against CODIS's "Unsolved Crimes Collection" unknown database).

their arms, or naturally shedding a strand of hair—is seemingly available for police collection without a Fourth Amendment warrant.[97] This is apparently so even though, "[l]ike little else, DNA is exposed to the public and abandoned every time we move."[98] Although the Supreme Court has not spoken definitively on this subject, and some scholars argue against treating such DNA as abandoned,[99] the matter has been deemed largely a non-issue by lower courts that have addressed it.[100] For instance, in *Raynor v. State*,[101] police took swabs of DNA from where the defendant had been "rubbing his bare arms against the armrests of the chair in which he had been seated."[102] During his unsuccessful challenge to the police's testing of that DNA, Raynor abandoned as fruitless any argument that the collection of his DNA from the armchair was unlawful.[103]

2. Privacy in the "Whole of a Person's Genetic Makeup": Levels 3, 4, and 5

The next three levels on the PAL chart involve criminal subjects who give DNA or test results to a third party—a company like 23andMe (Level 3) or a public website like GEDmatch (Level 4)—or to the police (Level 5). This Article will not discuss the Level 5 scenario because it assumes a criminal subject has made a knowing, voluntary waiver of any privacy rights after informed consent. Further, third-party ramifications of the searches at Levels 3 and 4 will be discussed in detail in Part IV in the context of the third-party doctrine, where they are most relevant. Instead, this section will focus entirely on whether, in light of the analysis in *Carpenter*, the Fourth Amendment should recognize a freestanding privacy interest in the "whole of a person's genetic makeup."

---

97 *See* Epstein, *supra* note 2, at 151–52.

98 *Id*. at 151.

99 *See generally* Albert E. Scherr, *Genetic Privacy & the Fourth Amendment: Unregulated Surreptitious DNA Harvesting*, 47 GA. L. REV. 445 (2013) (arguing against current case law that the Fourth Amendment should recognize a reasonable expectation of privacy in some "abandoned" DNA).

100 *See id.* at 447 n.1 (citing Commonwealth v. Bly, 862 N.E.2d 341, 351–52 (Mass. 2007)). *See also* State v. Christian, No. 04-0900, 2006 WL 2419031, at *1 (Iowa Ct. App. Aug. 23, 2006); State v. Athan, 158 P.3d 27, 31 (Wash. 2007).

101 99 A.3d 753 (Md. 2014), *cert. denied*, Raynor v. Maryland, 135 S. Ct. 1509 (2015).

102 *Id*. at 754.

103 *Id*. at 754–55.

3. Pre-*Carpenter* Considerations

Carpenter found a privacy interest under the Fourth Amendment in the "whole of a person's physical movements."[104] In recognizing that interest, the Court noted two guideposts from the Amendment: (1) securing "the privacies of life" against "arbitrary power," and (2) placing "obstacles in the way of a too permeating police surveillance."[105] Similarly, some argue an interest should be recognized in the content of one's DNA.[106] They see DNA as even more *sui generis* than cell phones and argue it should qualify for special protection because it contains "data that dwarfs the memory sticks of the average cell phone," is the "modern equivalent of the Domesday Book, an unalterable final survey of everything human," and is "even more revealing (present and future)" than the technology in *Riley* and *Carpenter*.[107] Moreover, *Ferguson v. City of Charleston*[108] provides support for a reasonable expectation of privacy in the test results of one's biological fluids (in that case, urine).[109] Essentially, supporters of a DNA privacy right argue for recognizing a privacy interest in the "whole of a person's genetic makeup."

Maryland rejected a similar argument in *Raynor v. State*, where police tested Raynor's "abandoned" DNA left on the armrest of an interview chair.[110] The court found that, while the "non-coding" DNA areas (i.e., "junk" DNA) are useful to identify a person, they do not give access to "intimate [genetic] information," and police have "no incentive" to go beyond identification.[111] And even if they did, Raynor did not have a reasonable expectation of privacy in the contents of his DNA (or at least the portion tested for identification).[112] This

---

104 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (drawing the phrase from opinions in *Jones v. United States*, 565 U.S. 400, 415, 430 (2012) (concurring opinions of Alito and Sotomayor, JJ., respectively)).

105 *Id.* at 2213–14.

106 Strutin, *supra* note 6, at 366 (wondering after *Riley* why the cell phone should receive more constitutional protections than the contents of the human body).

107 *Id.* at 361.

108 532 U.S. 67 (2001).

109 *Id.* at 80–86 (finding a violation when a state hospital adopted a policy to screen the urine of pregnant women for cocaine and refer them to police if they tested positive).

110 Raynor v. State, 99 A.3d 753, 755 (Md. 2014), *cert. denied*, Raynor v. Maryland, 135 S. Ct. 1509 (2015); *see also* Hana Gandi, *Why No Backlash?: Advances in Forensic Technology and the Criminalized Fourth Amendment*, 36 WHITTIER L. REV. 533, 552 (2015) (criticizing *Raynor*).

111 *Raynor*, 99 A.3d at 762.

112 *Id.* at 765.

reasoning tracked the Supreme Court's discussion in *King*.[113] The D.C. Circuit Court of Appeals also rejected a related argument in 2006.[114]

But both those cases were decided prior to *Carpenter*, both involved searches of CODIS, and neither involved a search into the more intimate data contained on private DNA databases.[115] In contrast, the Golden State Killer investigation searched for a genetic mutation.[116] Thus, a better argument can be made after *Carpenter*, especially if the searched DNA test results go beyond mere suspect identification.

Indeed, *Carpenter* provides new lines of argument. In recognizing a privacy interest in "the whole of a person's physical movements,"[117] the Court balanced five factors—"intimacy, comprehensiveness, expense, retrospectivity, and voluntariness"[118]—that apply in the context of DNA testing. This balancing was rightly criticized by the dissenters[119] but could be applied here as one of the alterations *Carpenter* made to Fourth Amendment law. This Article will apply the factors below, taking them at face value without questioning the wisdom of the Court in developing this multifactor test.

B. Applying Carpenter*'s Five Factors*

The first factor (Intimacy) recognizes that an activity is more likely to be protected by the Fourth Amendment if it provides an "intimate window into a person's life, revealing . . . 'familial, political, professional, religious, and sexual associations,'"[120] as well as a view into "private residences, doctor's offices, . . . and other potentially revealing locales."[121] Cell-site location information ("CSLI") met that criteria, and so might DNA results. Professor Sonia Suter explains that DNA invokes the intimate notion of "personhood"—it is "unique

---

[113] Maryland v. King, 569 U.S. 435, 464 (2013) (reasoning that "CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee" and are not tested for that purpose).

[114] *See* Johnson v. Quander, 440 F.3d 489, 498 (D.C. Cir. 2006) (rejecting the argument that police may not store a person's "genetic fingerprint" in CODIS and "re-search" it and concluding that accessing CODIS records is not a search because it matches "one piece of personal information against government records").

[115] *See generally id.*; *Raynor*, 99 A.3d 753.

[116] Oreskes et al., *supra* note 1.

[117] Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

[118] Justice Kennedy assigned these labels in dissent. *Id.* at 2234 (Kennedy, J., dissenting).

[119] *Id.* at 2234 (criticizing the Majority's "newly conceived" "multifactor analysis" as an "unstable foundation"); *see also id.* at 2272 (Gorsuch, J., dissenting) (lamenting that the new balancing test keeps *Smith* and *Miller* "on life support" while supplementing them with a "multilayered inquiry" that seems like "*Katz*-squared").

[120] *Id.* at 2217 (majority opinion) (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[121] *Id.* at 2218.

to each of us and therefore personal in the sense that it identifies us."[122] It too provides an intimate window into our lives: it "has a familial component, revealing links with relatives"; it "makes us vulnerable to undesirable exposure because it reveals intimate aspects of ourselves"; it can "stigmatize us" due to our "genetic flaws"; and it "makes us vulnerable to discrimination by insurers, employers, [and] future spouses."[123] Thus, although DNA does not reveal a person's movements, it does reveal the intimate (biological) essence of a person's nature.

The second factor (Comprehensiveness) recognizes that society's expectations about the comprehensiveness of law enforcement's capabilities can influence whether an expectation of privacy is objectively reasonable. For instance, society had an expectation "that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[124] With DNA, until the end of the last century, no one in society would have expected the decoding of the human genome and the ability of law enforcement to swab a cheek and comprehensively unlock the mysteries of a person's genetic makeup. That ability would have been in the realm of science fiction until recently. This factor also weighs in favor of recognizing a reasonable expectation of privacy in one's genetic makeup.

The third factor (Expense) recognizes that the greater the ease and inexpense with which the police can access private data "compared to traditional investigative tools," the greater the weight in favor of privacy rights.[125] As with the collection of CSLI, the efficiency of genetic testing (as demonstrated by the Golden State Killer case) makes it cheap and easy for law enforcement to upload a DNA sample on a free website (e.g., GEDmatch) and obtain previously unknowable leads to uncover a serial killer from decades ago.[126] Traditional investigative tools were woefully inept at finding the Golden State Killer, yet DNA tracking uncovered him with stunning alacrity. This factor also aligns in favor of recognizing a reasonable expectation of privacy.

The fourth factor (Retrospectivity) recognizes that a government intrusion with a "retrospective quality" that allows the police to learn past information about a criminal subject even before coming under investigation weighs in favor of privacy rights.[127] As *Carpenter* found with CSLI, DNA testing provides police an even more retrospective look into a criminal subject's past.

---

122 Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEO. WASH. L. REV. 737, 773 (2004).

123 *Id.* at 739.

124 *Carpenter*, 138 S. Ct. at 2217 (citing *Jones*, 565 U.S. at 430).

125 *Id.* at 2217–18.

126 Epstein, *supra* note 2, at 151–52 ("For DNA testing, the technology is not in the hands of private individuals but is easily obtained, at modest cost, from labs nationwide.").

127 *Carpenter*, 138 S. Ct. at 2218.

While DNA does not reveal the past movements of individuals, it does reveal the migrations of their ancestors, the true identity and biological history of their families, their genetic mutations, and their predisposition for future disease. In the process of searching for suspects using DNA databases, all this data can be uncovered on a person who is not even under the gaze of suspicion for any offense. This too weighs in favor of privacy.

The fifth factor (Voluntariness) recognizes that activities that are less voluntary—either because of societal factors (e.g., those who "compulsively carry cell phones with them all the time") or because of the nature of technology (e.g., "a cell phone logs a cell-site record by dint of its operation, *without any affirmative act on the part of the user beyond powering up*")—are more likely to be considered private.[128] In the context of genetic testing, DNA is shed by everyone all day long wherever they go, and the advances in technology make it ever more feasible to test that DNA. Also, DNA is often taken involuntarily (i.e., through arrest or conviction sampling requirements). Moreover, *Carpenter* clarified that the Fourth Amendment is not "surrendered" merely because a person ventures into the public sphere or because a private activity is "generated for commercial purposes."[129] Thus, the criminal subjects in Levels 3 and 4 of the PAL chart from Part II should not lose the ability to claim a protected privacy interest merely because they generated DNA results as part of commercial genealogy services or because they expected and welcomed some interaction in the public sphere.

Finally, *Carpenter* clarified that, when evaluating the issue, courts may consider the "continued increase in technology," including the "more sophisticated systems that are already in use or in development."[130] The *Carpenter* Court looked beyond the facts of the case from 2011 and ruled based on 2018 technology and beyond. One can only imagine what the future might hold for DNA research. Even "junk DNA" may one day have the potential to reveal intimate details about a person. Acting now to protect DNA under the Fourth Amendment makes as much sense as protecting the CSLI in *Carpenter*.

In sum, the Supreme Court in *King* (and several lower courts) did not seem amenable to recognizing a substantive privacy interest in a person's own genetic makeup. But those cases were limited to situations involving a CODIS search of "junk DNA" for mere identification purposes, with the government's assurance it was not interested in searching for any other type of genetic data. The private genealogy database question addressed in this Article raises the exact situations the Supreme Court was avoiding in *King* (and for which Justice Scalia derided the Majority). And after *Carpenter*—at least in a search of the criminal suspect's own DNA results generated by private companies—the five balancing

---

128 *Id.* at 2218, 2220 (emphasis added).

129 *Id.* at 2217.

130 *Id.* at 2218–19.

factors are more likely to weigh in favor of recognizing a privacy interest under the Fourth Amendment in the "whole of a person's genetic makeup."

1. Privacy in the DNA of a Biological Relative? Levels 6, 7, 8, and 9

In the prior two sections, this Article has contended that, under a *Katz* Fourth Amendment analysis (in light of *Carpenter* and advancing technology), individuals have a reasonable expectation of privacy in the contents of their DNA, whether it is in their body, in their personal possession, or even out of their possession (subject to the third-party doctrine, to be discussed in Part IV).

But perhaps the most intriguing aspect of this issue is the way law enforcement has located suspects by searching private genealogy databases for the suspects' biological relatives (i.e., "familial searching").[131] That is the situation with Levels 6, 7, 8, and 9 of the PAL chart—it is the biological relatives of the criminal subject whose own DNA or test results are either within their possession (Level 6) or given to a third party (Level 7), a public website (Level 8), or the police (Level 9). These four levels will be analyzed together below for reasons that will become apparent.

In the usual scenario, law enforcement—armed with an unknown DNA sample—searches a private genealogy DNA database and discovers a DNA test result that matches a biological relative of the unknown sample's owner.[132] The police then use that DNA information to narrow down the list of potential suspects, eventually discovering the identity of the actual perpetrator through the use of other investigative means and techniques.[133] In this process, what privacy interests are implicated? As one commentator noted, this creates a "fourth-party problem of sorts" because it raises the question of whether a criminal suspect has any legal interest in a family member's DNA that has been uploaded to a commercial DNA database.[134]

Adding yet another wrinkle, it may be impossible for the police to prevent the actual suspect's DNA from exposure during one of these "biological relative" database searches.[135] A broad search of a database for the relative of a suspect might very well reveal the suspect's own DNA data because in these familial searches "the word 'relative' can refer to 'the person in the database, any

---

131 Murphy, *supra* note 57, at 297–98 (explaining "when a database search does not turn up an exact match, it is possible to follow up with a moderate- or low-stringency search that returns partial matches—profiles that match some, but not all, of the sample's alleles"—usually up to 25 persons).

132 *See, e.g.*, *supra* note 4 and accompanying text.

133 *See, e.g.*, *id.*

134 Ford, *supra* note 15.

135 *See, e.g.*, Murphy, *supra* note 57, at 298.

of that person's kin (suspected sources of the material), as well as the actual source of the material.'"[136]

To simplify the analysis, this Article will assume the police can search a genealogy database and find a relative without uncovering the DNA results of the actual suspect. Given that caveat, does a suspect have a "reasonable expectation of privacy" in the DNA of a distant relative (or a close relative, for that matter)? Put another way, does the suspect have a personal privacy interest in the genetic material coming from a relative's body? The answer to that question is "no."[137]

The primary problem is "standing"—a doctrine that "focuses on whether the person seeking to challenge the legality of a search as a basis for suppressing evidence was himself the 'victim' of the search or seizure."[138] "The Supreme Court's expectation of privacy cases deny standing to other family members, as Fourth Amendment rights are deemed 'personal.'"[139] The Court has held that personal rights "may not be vicariously asserted," and therefore a person who had damaging evidence found "by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed."[140] Here, criminal subjects who seek to apply the exclusionary rule to suppress evidence obtained through the search of DNA samples of biological relatives are attempting to vicariously assert the rights of their third-party relatives. The subjects are not the victims. The only ones who could raise an objection would be the biological family members themselves.

A way of addressing the standing problem here is to simply recognize that a person does not—subjectively or objectively—have an expectation of privacy in someone else's body. While that should end the matter, after *Carpenter* it is fair to ask whether a right to the "whole of a person's genetic material" might be stretched to include "genetic material held in common with a relative." If someone else's DNA can reveal private data about criminal subjects, one might argue the subjects have some expectation that their portion of the DNA will remain private (at least from the police).

---

136 *Id.* at 298.

137 *See id.* at 334 ("What constitutional interest does the lawfully databased person, or that person's relatives, have in that search? . . . [U]nder conventional doctrine, none.").

138 Rakas v. Illinois, 439 U.S. 128, 132 (1978).

139 Epstein, *supra* note 2, at 161–62. Professor Epstein cites several articles critical of this doctrine, including Elwood Earl Sanders, Jr., *Fourth Amendment Standing: A New Paradigm Based on Article III Rules and Right to Privacy*, 34 CAP. U. L. REV. 669, 681 (2006) (arguing to broaden the standing doctrine to include "anyone against whom the evidence is being introduced").

140 *Rakas*, 439 U.S. at 133–34. The doctrine partly stems from the Court's desire to limit the use of the Fourth Amendment's exclusionary rule only to benefit those whose rights have been violated. "Even if such a person is not a defendant in the action, he may be able to recover damages for the violation of his Fourth Amendment rights or seek redress under state law for invasion of privacy or trespass." *Id.* at 134.

The problem with this theory is twofold. Subjectively, it seems implausible most people believe they have a privacy interest in biological data contained in the body of a relative (who they might never have met). Even if such a person with that subjective belief could be found, objectively—although there is no objective data to support this next statement—it seems society would not be willing to go that far in recognizing such an asserted privacy right as reasonable. To ask the question is nearly to answer it because it seems so far removed from any current societal beliefs. It is unlike the dubious, but now-accepted, proposition under *Katz* that "individuals can have a reasonable expectation of privacy in another person's property."[141]

Indeed, the Supreme Court's abortion precedents involving the right of privacy have made it clear that one person (i.e., the father) does not have an actionable privacy interest in the body of another person (i.e., the mother of the father's child) while that child is within the mother's womb.[142] And if a father does not have an actionable privacy interest in that circumstance, it seems unlikely a relative could assert a constitutionally protected privacy interest in the DNA of another.[143] Moreover, such an assertion would be difficult to control with any reasonable limiting principle, since 99.7% of genetic material is also shared with every other person on the planet. In light of that statistic, at what point would such a privacy interest cease?

For those reasons, a *Katz* analysis under the circumstances in Levels 6, 7, 8, and 9 of the PAL chart leads to the conclusion that a criminal subject has no reasonable expectation of privacy in the DNA or test results of a biological relative. In sum, while criminal subjects of a police genealogy search might be able to assert a Fourth Amendment privacy interest in their own DNA or test results (subject to the third-party doctrine), they have no right to assert the privacy interests of biological relatives, whose DNA might be exposed to police intrusion as part of a familial search.

---

[141] Carpenter v. United States, 138 S. Ct. 2206, 2242 (2018) (Thomas, J., dissenting) ("[A] person may have a legitimate expectation of privacy in the house of someone else." (citing Minnesota v. Carter, 525 U.S. 83, 89 (1998)).

[142] *See* Planned Parenthood v. Casey, 505 U.S. 833, 838 (1992) (striking down a provision requiring woman to notify husband of abortion decision, stating "it cannot be claimed that the father's interest in the fetus' welfare is equal to the mother's protected liberty, since it is an inescapable biological fact that state regulation with respect to the fetus will have a far greater impact on the pregnant woman's bodily integrity than it will on the husband"); Roe v. Wade, 410 U.S. 113, 165 n.67 (1973) ("Neither in this opinion nor in *Doe v. Bolton* . . . do we discuss the father's rights, if any exist in the constitutional context, in the abortion decision. No paternal right has been asserted in either of the cases . . . .").

[143] *See also* Greely et al., *Family Ties: The Use of DNA Offender Databases to Catch Offenders' Kin*, 34 J.L. MED. & ETHICS 248, 257–58 (2006) (arguing Due Process does not give a parent the right to challenge the search of a child's DNA, even though a parent has a right to control a child's upbringing and education).

C. Analyzing Genetic Privacy Under the Traditional Property-Rights Approach

The Supreme Court recently has sought to restore the traditional pre-*Katz* property-rights analysis under the Fourth Amendment. But would applying a property-based analysis in the DNA context lead to a different result than a *Katz* analysis? Referencing the various privacy levels in the PAL chart at the end of Part II, this section addresses that question.

1. Restoring a Traditional Property-Based Approach to the Fourth Amendment

In *Jones*, the Supreme Court signaled its desire to restore the traditional property-based approach to its rightful analytical place under the Fourth Amendment because the Court had unwittingly displaced it by the *Katz* analysis.[144] Justice Scalia explained the Court's Fourth Amendment cases had been tied to common-law trespass "at least until the latter half of the 20th century," but that its jurisprudence had "deviated from that exclusively property-based approach" beginning with *Katz*.[145] He observed that *Katz* merely had "established that 'property rights are not the sole measure of Fourth Amendment violations,' but did not 'snuf[f] out the previously recognized protection for property,'" and that *Katz* "did not erode the principle 'that, when the Government does engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'"[146]

The *Carpenter* Court did not use a property-based approach in finding a privacy interest in the "whole of a person's movements," and the dissenters accused the Majority of "unhing[ing] Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic framework that pertains in these cases."[147] These dissents are most appropriately discussed in Part IV (when evaluating the third-party doctrine), but one dissenting view is helpful to discuss in this section of the Article. Justice Gorsuch's dissent in *Carpenter* offered "another way" of re-envisioning the Court's cases under *Katz* using the traditional property-based approach, recognizing that it might extend more rights than the historically inconsistent results of the "reasonable expectation of privacy" approach. Justice Gorsuch—having taken Justice Scalia's seat after his death—seems to have taken up the late Justice's mantle in restoring (or revolutionizing) that traditional property-based approach.

---

144 *See* United States v. Jones, 565 U.S. 400, 405–07 (2012).

145 *Id.* at 405.

146 *Id.* at 407 (emphasis omitted) (citing Soldal v. Cook Cty., 506 U.S. 56 (1992) and United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)).

147 Carpenter v. United States, 138 S. Ct. 2206, 2224 (2018) (Kennedy, J., dissenting).

In the context of the facts in *Carpenter*, for instance, Justice Gorsuch called it "entirely possible" that "a person's cell-site data could qualify as his papers or effects under existing law" despite that "the telephone carrier holds the information," because various federal laws give customers "substantial legal interests" and "certain rights to control use of and access to" CSLI, including a federally created "private cause of action for damages against carriers who violate" those laws.[148] But Justice Gorsuch lamented that "we do not know anything more" in the record because Carpenter had forfeited any property-based arguments by failing to raise them before the lower courts: "In these circumstances, I cannot help but conclude—reluctantly—that Mr. Carpenter forfeited perhaps his most promising line of argument."[149]

Some scholars see Justice Gorsuch's opinion as "the most important aspect of *Carpenter*" for those "who have long been frustrated by the Fourth Amendment's bizarre reasonable-expectation-of-privacy test," with a bold prediction that "*Carpenter* represents the beginning of what will likely be a growing shift away from *Katz* and its progeny."[150] But in the context of DNA testing, could the property-based approach truly provide the same or greater rights to criminal subjects as that provided under *Katz*? That is the question for the remainder of this section.

2. Property Interest in One's Own DNA: Levels 1 through 5

Earlier, this Article argued the *Katz* analysis would yield a "reasonable expectation of privacy" in one's own DNA and test results because society was willing to recognize an objective expectation that one's own DNA will not be plundered by the police, especially while it is in one's own body or personal possession. It also suggested the not-yet-established proposition that a freestanding privacy interest in the "whole of a person's genetic makeup" might be recognized as objectively reasonable by society in light of the balancing factors articulated in *Carpenter*. A property-based analysis could reach a similar result via a different route.

To find recognition under the Fourth Amendment, the Court has traditionally looked to positive law and the common law to establish whether an individual has any property rights in a particular interest. In their joint *Carpenter* dissent, Justices Samuel Alito and Clarence Thomas explained how a traditional property-based approach would proceed: the Court would "first ask[] whether the object of the search—say, a house, papers, or effects—belonged to the

---

148 *Id.* at 2272 (Gorsuch, J., dissenting).

149 *Id.*

150 Trevor Burrus & James Knight, Katz *Nipped and* Katz *Cradled:* Carpenter *and the Evolving Fourth Amendment*, 2018 CATO SUP. CT. REV. 79, 110–11 (2017–2018).

defendant, and, if it did, whether the Government had committed a 'trespass' in acquiring the evidence at issue."[151]

Using that analysis here, the Court would first identify the object of the search—in this case, a person's DNA or the results of a DNA test—and then determine whether that object belonged to the defendant. Therefore, the question posed would be whether an individual has a property interest in their own biological cells and the results of testing done on those cells. Although some Supreme Court Justices have expressed doubt about property interests in "abandoned" bodily fluids,[152] after *Carpenter* the answer to that question may be "yes" for three reasons.

First, as a matter of positive law, some legislatures recognize property interests associated with DNA and test results, declaring them to be the property of the individual.[153] For instance, Florida decrees "the results of . . . DNA analysis, whether held by a public or private entity[, to be] the exclusive property of the person tested."[154] These declarations of positive law—though currently in a minority of states—indicate that ownership rights in DNA and test results may be enforceable property interests. As Justice Gorsuch discussed in his *Carpenter* dissent, "positive law may help provide detailed guidance on evolving technologies without resort to judicial intuition" because legislatures "often create[] rights in both tangible and intangible things."[155]

Second, the genealogy companies themselves recognize that property and contract law ascribe ownership rights, as a general matter, to those users who submit DNA to their sites. For instance, according to the terms of service governing Ancestry's customers, those who submit their DNA "always maintain ownership of [their] data," and Ancestry must get their informed consent prior to

---

151 *Carpenter*, 138 S. Ct. at 2259 (Alito, J., dissenting) (citing United States v. Jones, 565 U.S. 400, 411 (2012)).

152 *See* Ferguson v. City of Charleston, 532 U.S. 67, 92 (2001) (Scalia, J., dissenting) (emphasis omitted) (joined by Rehnquist, C.J., & Thomas, J.) ("I suppose the testing of that urine for traces of unlawful drugs could be considered a search of sorts, but . . . it is entirely unrealistic to regard urine as one of the 'effects' (i.e., part of the property) of the person who has passed and abandoned it.").

153 Colorado and Georgia recognize that "genetic information is the unique property of the individual" who is tested (and to whom the information pertains). COLO. REV. STAT. ANN. § 10-3-1104.7(1)(a) (West 2019); GA. CODE ANN. § 33-54-1 (West 2019). Alaska legislates that "a DNA sample and the results of a DNA analysis performed on the sample are the exclusive property of the person sampled or analyzed." ALASKA STAT. ANN. § 18.13.010(a)(2) (West 2019). Louisiana explains that "genetic information is the property of the insured or enrollee. No person shall retain an insured's or enrollee's genetic information without first obtaining authorization." LA. STAT. ANN. § 22:1023(E) (West 2019). Other states are considering similar legislation.

154 FLA. STAT. ANN. § 760.40(2)(a) (West 2019).

155 *Carpenter*, 138 S. Ct. at 2270 (Gorsuch, J., dissenting). But Justice Gorsuch noted one limitation: "[W]hile positive law may help establish a person's Fourth Amendment interest there may be some circumstances where positive law cannot be used to defeat it." *Id.*

conducting research on submitted DNA.[156] Ancestry's terms of service also state, "You own your Personal Information, Additional User Information, and User Provided Content," and they require their customers to grant Ancestry "the right to collect, host, transfer, process, analyze, communicate and store your Personal Information (including your Genetic Information) and Additional User Information" to provide the sites' genealogy services.[157] While 23andMe's terms are not as explicit (or as generous to its customers), they do reflect an understanding that their users have rights (to waive).[158] And publicly available genealogy sites, such as GEDmatch, also ascribe property interests to their customers. As GEDmatch's terms acknowledge, "Raw DNA data uploaded to GEDmatch.Com ('Raw Data') remains the property of the person who uploaded it."[159] Moreover, GEDmatch recognizes that the owner of the results has the ability to remove them from the website at any time, thus preventing further use of the test results by the site.[160]

Third, even where positive law does not expressly define a property interest in DNA and test results, courts may look to broader property-law concepts to determine the existence of that interest. For instance, in the 1990 California Supreme Court decision, *Moore v. Regents of the University of California*,[161] the court concluded a patient did not have a valid claim for the tort of conversion because he did not retain a sufficient property interest in cells removed from his body and used for research without his consent.[162] The Majority did, however, recognize a property right in those cells still in the patient's body, even though it did not find sufficient precedent at that time to establish a continuing ownership right once the cells were removed.[163]

---

156 *Ancestry Terms and Conditions*, ANCESTRY (July 25, 2019), https://www.ancestry.com/cs/legal/termsandconditions.

157 *Id.*

158 *See 23andMe Terms and Conditions*, 23ANDME, https://www.23andme.com/about/tos/ (last visited Aug. 29, 2019). According to the terms:

> Waiver of Property Rights: You understand that by providing any sample . . . you acquire no rights in any research or commercial products that may be developed by 23andMe or its collaborating partners. You specifically understand that you will not receive compensation for any research or commercial products that include or result from your Genetic Information or Self-Reported Information.

159 *GEDmatch.Com Terms of Service and Privacy Policy*, *supra* note 86.

160 *Id.* GEDmatch explains the process to deny the site further use of the property: "A link or other means is provided within your GEDmatch account to remove your Raw Data from the Site. Alternatively, you can request deletion of your personal information at any time . . . ." *Id.*

161 793 P.2d 479 (Cal. 1990).

162 *Id.* at 488–97.

163 *See id.* at 493 ("[W]e do not purport to hold that excised cells can never be property for any purpose whatsoever.").

In dissent in *Moore*, Justice Stanley Mosk discussed the broader property-law issues that could undergird an argument in favor of finding a general property interest. He observed that "concepts of property and ownership" are extremely broad and include "everything which one person can own and transfer to another" and "every species of right and interest capable of being enjoyed as such upon which it is practicable to place a money value."[164] He explained that property refers to a "bundle of rights and privileges as well as of obligations"[165]—principally "the rights to possess the property, to use the property, to exclude others from the property, and to dispose of the property by sale or by gift."[166] Thus, even if the law "limits or even forbids the exercise of certain rights over certain forms of property," other rights in the bundle might persist and "what remains is still deemed in law to be a protectible property interest."[167] He concluded that, in the absence of any authority negating the claimed property right in the excised cells, "the right falls within the traditionally broad concept of property in our law."[168] Justice Mosk's argument, though in dissent in that case, provides a strong basis for the further claim that—even in the absence of positive law—a court could recognize a property interest based on evidence demonstrating the presence of some or all of the tell-tale "bundle of rights."

Here, as the terms of service from genealogy sites illustrate, the owner of DNA samples and test results may negotiate for some remuneration for the company to access test result data or compare their DNA sample to others, whether for research, patent development, or some other commercial purpose. That these companies require waivers from their customers, including waivers of rights in potential patents and other intellectual property products, indicates the DNA and test results have a marketable value. The weight of the evidence demonstrates that both the DNA sample and the results of a DNA test possess the characteristics of the "bundle of rights" associated with property ownership. For instance, by denying consent for research, the owner of the DNA test results can prevent Ancestry from using those results in research. And by removing data from GEDmatch, the owner can prevent the site from its further use. Finally, some broker websites already offer money for DNA samples.[169]

---

164 *Id.* at 509 (Mosk, J., dissenting) (quoting Yuba River Power Co. v. Nev. Irrigation Dist., 279 P. 128 (Cal. 1929)).

165 *Id.* at 509 (quoting Union Oil Co. v. State Bd. of Equalization, 386 P.2d 496, 500 (Cal. 1963)).

166 *Id.* at 509.

167 *Id.* at 509–10.

168 *Id.* at 510.

169 Companies are already trading DNA samples for cash. *See* Ali Montag, *This Company Will Pay You $50 for Your Spit—and Mark Cuban Just Invested $200,000 on 'Shark Tank'*, CNBC MAKE IT (Nov. 13, 2017), https://www.cnbc.com/2017/11/13/mark-cuban-invested-200000-in-dna-simple-on-shark-tank-heres-why.html; *How Much Money Can You Make Selling Your DNA?*,

Once the existence of a property right in one's DNA and test results is accepted, the final step in the Fourth Amendment analysis is to determine "whether the Government had committed a 'trespass' in acquiring the evidence at issue."[170] The value of the property interest here—the DNA and its test results—are the contents themselves. Thus, any intrusion into the contents of the tests (which, in turn, reveals the contents of the DNA) could be considered a trespass. Conducting a search of a database containing the property of criminal subjects and accessing the raw data of their DNA test results to compare with other samples (for identification or other purposes) would be a clear trespass on the claimed property interests, resulting in a Fourth Amendment violation unless some authorization exists (such as a third-party issue, discussed in Part IV, or the presence of a warrant or warrant exception showing reasonableness).

3. Property Interest in Another's DNA: Levels 6 through 9

The prior section used a traditional property-based approach to the Fourth Amendment and established a more direct and perhaps stronger argument than *Katz* to recognize a privacy interest in one's DNA and test results. But property law would not support the type of claim presented in Levels 6 through 9 of the PAL chart, where the claimed property interest involves DNA belonging to another person. No accepted principle of property law would support the notion that one person "owns" another person's DNA as a matter of natural right.

Professor Erin Murphy has attempted to articulate a theory that might be applicable in this context, although it is mostly an argument under *Katz*. Her argument focuses on the rights of biological relatives who have been identified through a familial DNA search as relatives of a suspected criminal, and the impact on their lives and intrusion into their privacy by being associated with the suspected criminal.[171] She suggests these family members might have a "protectable interest in the privacy of their half of the databased kin's genetic code."[172] The theory would be that the family member "has a protected right not to have her own genetic information exposed, if you will, by the fact of her kin's conviction. Such an interest could be likened to the joint interest held by property owners who share common space,"[173] as in a situation where two condo owners

---

ENCRYPGEN, https://encrypgen.com/how-much-money-can-you-make-selling-your-dna/ (last visited Aug. 29, 2019) (explaining EncrypGen is "poised to . . . tip the scales in favor of the consumer/DNA data holder by putting them in control of their personal genomic data and allowing them to be paid for sharing their DNA rather than surrendering it to the testing companies").

170 Carpenter v. United States, 138 S. Ct. 2206, 2259 (2018) (Alito, J., dissenting).

171 *See* Murphy, *supra* note 57, at 336.

172 *Id.* at 336.

173 *Id.* Murphy goes on to argue that "the partial match search, and the inference drawn from the match itself, invoke constitutional scrutiny because they intrude on the legitimate expectation of privacy held by the relative in her half of the offender's genetic code, and are impermissible because they do so without individualized or particularized suspicion." *Id.* at 337.

in the same condominium share a common area in which they have a shared interest. If Professor Murphy's argument has validity, then it could be applied in both directions. For instance, the criminal subject's DNA would also be "exposed" to the public insofar as it is matched to the biological relative's sample. The subject could then make the identical argument as the family member, in reverse.

But the argument is problematic. The analogy of a "joint interest held by property owners who share common space" conflates the geographic areas involved. The analogy in the DNA context would not be two condo owners who share a common space in the same condominium. Instead, the analogy would be two condo owners who each live and own a condo in separate complexes, except that the common-area floorplans are identical in both condos. (Perhaps they were built by the same developer.) No property-law principle would allow the owner in one condo to have legal say in the affairs of the other condominium, no matter how identical the common-area floorplans. Therefore—to a much lesser extent than under a *Katz* analysis—the traditional property-based approach would not support an argument affirming a property interest in another person's DNA.[174] There would be no personal Fourth Amendment interest at stake, and standing limits again would prevent the criminal subject from vicariously asserting the property rights of a third party.

In sum, both the *Katz* and property-based analyses reach similar results, as discussed in this Part. Both can be used to put forward a plausible argument that the Fourth Amendment should protect the interests of a person in their own DNA and test results, even when those results are in the possession of others (setting aside until Part IV the issue of the third-party doctrine). And both theories should not be interpreted to support an attempt to claim a natural privacy interest in the DNA or test results of another person.

IV. GENETIC PRIVACY AND THE THIRD-PARTY DOCTRINE AFTER *CARPENTER*

Part III of this Article concluded that criminal subjects whose DNA or test results were searched by the government likely would be protected by the Fourth Amendment with regard to their own DNA, but not so for the DNA results of biological relatives. Throughout the discussion, the issue of the third-party doctrine was deferred for later analysis, even though the outcome of that question could very well negate the privacy interest provisionally recognized above. Now, Part IV of this Article addresses the doctrine after *Carpenter*. First, it explains the history of the third-party doctrine and how the *Carpenter* Court cabined the

---

[174] *See Carpenter*, 138 S. Ct. at 2247 (Alito, J., dissenting) (criticizing the Majority's "destabiliz[ing]" reasoning under *Katz*, calling it "revolutionary" that the Court would allow a defendant "to object to the search of a third party's property"). Any theory that might allow this type of claim here would come under *Katz*, as in *Carpenter*, and not the traditional property-based approach. *See supra* Section III.A.

doctrine for future Fourth Amendment cases. Then, this Part examines whether the Court would use the same reasoning as in *Carpenter* to place limitations on the third-party doctrine in the context of DNA testing. During the discussion, it will analyze the doctrine from both a *Katz*-based and property-based approach to the Fourth Amendment.

A. The Third-Party Doctrine and the Carpenter *Decision*

This section outlines the history of the third-party doctrine and how *Carpenter* might have changed that doctrine for the future where new technologies are involved. It explores the basis of the doctrine through the eyes of the *Carpenter* Court and examines the alternative positions of some of the dissenting Justices.

1. The History of the Third-Party Doctrine

After *Katz*, with the Supreme Court expanding its Fourth Amendment jurisprudence to include "reasonable expectations of privacy," the Court's new direction had the potential to disrupt the effectiveness of law enforcement by placing restrictions on common investigative techniques (e.g., tracking money transactions made through financial institutions), surreptitious surveillance (e.g., tracking phone numbers dialed through the switchboard), and undercover operations (e.g., recruiting informants and wiring them to record incriminating conversations). Because none of these law enforcement practices involved a trespass on the property of a suspect, traditional notions of the Fourth Amendment had not triggered its protections. But all of that changed with *Katz* because defendants could now argue they reasonably believed their bank records would be kept private, the phone numbers they dialed would not be recorded, and their conversations would not be taped.

These police techniques had one thing in common: the cooperation of a third party (a bank, a telephone company, an informant). Enter the third-party doctrine, which generally holds that, by disclosing information to a third party, "the subject gives up all of his Fourth Amendment rights in the information revealed."[175] The Court first articulated the doctrine in *United States v. Miller*,[176] which upheld a police subpoena of Miller's banks records, gathering "several months of canceled checks, deposit slips, and monthly statements."[177] By revealing his affairs to a third party (the bank), Miller had assumed the risk the bank might convey his personal data to the police.[178] In explaining *Miller*, the

---

[175] Ormerod & Trautman, *supra* note 20, at 110–11 (discussing the third-party doctrine's origins in cases such as *On Lee v. United States*, 343 U.S. 747 (1952)).

[176] 425 U.S. 435, 443 (1976).

[177] *Carpenter*, 138 S. Ct. at 2216 (explaining the significance of *Miller*).

[178] *Id.*

Carpenter Court listed three reasons Miller had no privacy interest in the bank records: he could "assert neither ownership nor possession" of the records because "they were 'business records of the banks'"; the checks were "not confidential communications but negotiable instruments to be used in commercial transactions"; and "the bank statements contained information 'exposed to [bank] employees in the ordinary course of business.'"[179] It did not matter that Miller assumed the bank would use his personal information solely for a limited purpose.[180]

The Supreme Court expanded the third-party doctrine in *Smith v. Maryland*,[181] which upheld police use of a "pen register—a device that recorded the outgoing phone numbers dialed on a landline telephone"—because Smith assumed the risk when he conveyed the dialed numbers to the phone company.[182] In explaining *Smith*, the *Carpenter* Court detailed three reasons Smith had no reasonable expectation of privacy in the numbers he dialed on his phone: a pen register has "limited capabilities"; it is doubtful "people in general entertain any actual expectation of privacy in the numbers they dial"; and telephone subscribers know "the numbers are used by the telephone company 'for a variety of legitimate business purposes,' including routing calls."[183]

After *Katz*, the Court continued to approve the police use of informants under an assumption-of-risk theory, even where the informant gained the defendant's trust to enter into his home or recorded conversations wearing a wire.[184] As Justice Scalia later quipped, "Abuse of trust is surely a sneaky and ungentlemanly thing, and perhaps there should be (as there are) laws against such conduct by the government. . . . That, however, is immaterial" because a person's misplaced trust in a colleague is "not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities."[185]

As new technologies arose, courts expanded the third-party doctrine to approve police operations intercepting other information held by third parties: "subscriber information, the length of . . . stored files, . . . and a sender's name, email address, and [internet protocol] address."[186] Even as the doctrine expanded,

---

179 *Id.* (citations omitted).

180 *Id.*

181 442 U.S. 735, 743–44 (1979).

182 *Carpenter*, 138 S. Ct. at 2216 (explaining the significance of *Smith*).

183 *Id.* (citations omitted).

184 *See* United States v. White, 401 U.S. 745, 749 (1971); Hoffa v. United States, 385 U.S. 293 (1966).

185 Ferguson v. City of Charleston, 532 U.S. 67, 94 (2001) (Scalia, J., dissenting) (citing *White*, 401 U.S. at 749).

186 Sarah Wilson, *Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals When Third Parties Are Forced to Hand Over Passwords*, 30 BERKELEY TECH. L.J. 1, 17 (2015).

preserving the ability of police to continue normal operations, the Supreme Court warned that the doctrine had limits. The Court drew a key distinction between the permissible interception of "non-content" information—items noted above—and the prohibited interception of "content" data, such as the substance of phone conversations, the content of messages, and "items that are not directed to the third-party intermediary (such as the [internet service provider]), but rather to a specific recipient."[187] And in certain instances the Court ignored the doctrine entirely due to other privacy concerns.[188]

The third-party doctrine has been criticized as "dead wrong," "a mockery of the Fourth Amendment," "among the most maligned constitutional doctrines," and "one of the most serious threats to privacy in the digital age."[189] Some worry about the "chilling effect" that "stem[s] from anxiety about where sensitive information, once collected, might flow."[190] Others believe the Supreme Court never articulated a "clear argument in its favor," with some finding the doctrine to be "unexplained" or merely results-oriented.[191] In *United States v. Jones*, Justice Sotomayor questioned if the doctrine could survive in a digital age where people "reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[192] Even a newly-appointed Justice Gorsuch joined the chorus of critics, contending the Court has "never offered a persuasive justification" for the third-party doctrine, and that it could lead to the demise of the Fourth Amendment in the digital age.[193]

By the time of *Carpenter*, some believed the doctrine had outlived its usefulness.

2. The Impact of the *Carpenter* Decision

Carpenter finally put the brakes on the third-party doctrine in the face of evolving technology, refusing to "mechanically" apply the doctrine to cell-site location information (CSLI), a "distinct category of information."[194] Yet the

---

187 *Id.* at 17.

188 *See Ferguson*, 532 U.S. at 84–85 (invalidating state hospital policy where pregnant women "entrusted" their urine to doctors, who later gave urinalysis results to police if they tested positive for cocaine); *see also* Ormerod & Trautman, *supra* note 20, at 115–16 (discussing *Ferguson*).

189 Ormerod & Trautman, *supra* note 20, at 113 (citations omitted).

190 Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 U. KAN. L. REV. 485, 497 (2018).

191 Ormerod & Trautman, *supra* note 20, at 113–14 (citations omitted).

192 United States v. Jones, 565 U.S. 400, 417 (Sotomayor, J., concurring).

193 Carpenter v. United States, 138 S. Ct. 2206, 2262–63 (2018) (Gorsuch, J., dissenting) ("What's left of the Fourth Amendment? . . . Countless Internet companies maintain records about us and, increasingly, for us. Even our most private documents . . . now reside on third party servers." (emphasis omitted)).

194 *Id.* at 2219 (majority opinion).

Court purportedly did not overturn the third-party doctrine, opting instead to "decline to extend" it under the unique circumstances of the case.[195]

The Court gave two reasons for rejecting the doctrine's application in *Carpenter*. First, the primary rationale for the third-party doctrine—i.e., only limited information can be gleaned from data such as telephone numbers or publicly negotiable checks—did not apply to CSLI, which "implicates privacy concerns far beyond those considered in *Smith* and *Miller*" and involves "seismic shifts in digital technology" that make it possible to track the location of "everyone . . . for years and years."[196] But in dissent, Justice Kennedy saw CSLI as "no different from the many other kinds of business records the Government has a lawful right to obtain" through the subpoena process.[197]

Second, the Court concluded that the assumption-of-risk rationale—i.e, that "information knowingly shared with another" creates a "reduced expectation of privacy"—did not apply because CSLI "is not truly 'shared' as one normally understands the term" due to the "indispensable" requirement to carry a cell phone for "participation in modern society" and because cell phones log location data "without any affirmative act on the part of the user beyond powering up," thus defeating the notion the user "assumed the risk" in any "meaningful sense."[198]

One key argument made by the dissenting Justices was that the Majority had created instability with regard to the subpoena power.[199] Justice Alito gave an in-depth analysis of the subpoena issue,[200] while Justice Kennedy pointed out perceived absurdities in the Court's holding.[201] Justice Kennedy contrasted warrants, which allow "the Government to enter and seize and make the examination itself," with subpoenas that "simply require[] the person to whom it is directed to make the disclosure. A subpoena, moreover, provides the recipient

---

195 *Id.* at 2220.

196 *Id.* at 2219–20.

197 *Id.* at 2224 (Kennedy, J., dissenting). Kennedy contended financial and telephone records pose as great a danger as CSLI, disclosing "how much money they make; the political and religious organizations to which they donate; whether they have visited a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center; whether they go to gay bars or straight ones; and who are their closest friends and family members." *Id.* at 2232.

198 *Id.* at 2219–20 (majority opinion).

199 *See id.* at 2247–57 (Alito, J., dissenting); *id.* at 2224–32 (Kennedy, J., dissenting).

200 *Id.* at 2247–57 (Alito, J., dissenting) (discussing the Majority's mistake on the subpoena issue in depth).

201 *Id.* at 2224 (Kennedy, J., dissenting) (deriding the Majority's view that "the Government can acquire a record of every credit card purchase and phone call a person makes over months or years without upsetting a legitimate expectation of privacy," but that it cannot obtain "a court's approval to issue a subpoena for more than six days of cell-site records in order to determine whether a person was within several hundred city blocks of a crime scene").

the 'opportunity to present objections' before complying, which further mitigates the intrusion."[202]

Some scholars see in *Carpenter* the beginning of a broader rethinking of the Fourth Amendment, especially the third-party doctrine. The decision shows the Court is "willing to reconsider old doctrines that do not fit with the realities of the digital age," and it "frees lower courts from the dead hand of *Smith* and *Miller* to protect data of comparable 'depth, breadth, and comprehensive reach' to CSLI."[203] Others are skeptical that *Carpenter* will have significant impact on the doctrine, recognizing that the Court's holding is "fairly narrow and unique to cell-site location information," due to the "ubiquity of cell phones."[204] Some find it unlikely the case will "extend Fourth Amendment protections to the acquisition and utilization of other digital identifiers and tracers, such as Internet Protocol ('IP') addresses and general forms of metadata."[205]

B. Applying the Third-Party Doctrine to Genealogy Websites

This section applies the third-party doctrine after *Carpenter* in the context of private genealogy websites, such as Ancestry and 23andMe, and publicly available sites such as GEDmatch, which has often been used by law enforcement to track down relatives of suspected criminals. It first explains how these sites work from the perspective of individuals handing over their intimate DNA data to third parties. Returning to the PAL chart from Part II, this section then explores whether the post-*Carpenter* third-party doctrine will negate Fourth Amendment privacy interests in the DNA context. Discussion will focus solely on PAL Levels 3 and 4, where individuals provide their own DNA or test results to third parties—either a private company, such as Ancestry (Level 3), or a publicly available website, such as GEDmatch (Level 4).

1. Information Given to Genealogy Websites

Assuming individuals have a protected Fourth Amendment privacy interest in their own DNA and the results of DNA testing—either through a traditional property-based analysis or the modern *Katz* approach—the question then becomes whether that privacy interest is defeated through application of the

---

202 *Id.* at 2228.

203 Michael Price, *Carpenter v. United States and the Future Fourth Amendment*, CHAMPION, June 2018, at 48, https://www.nacdl.org/Article/June2018-Carpenterv-UnitedStatesandtheF.

204 Blake A. Klinkner, *In Ruling that Cell Phone Tracking Information Is Subject to 4th Amendment Warrant Requirements, the U.S. Supreme Court Hopes Not to "Embarrass the Future"*, WYO. LAW., Aug. 2018, at 54–55, http://digitaleditions.walsworthprintgroup.com/publication/?i=516222&p=&l=&m=&ver=&view=&pp=#{%22issue_id%22:516222,%22page%22:56.

205 *Id.*

third-party doctrine. To help assess this question in the context of genealogy websites, it is critical to determine what information is passed to these third parties and under what limitations, if any. This is so because scholars have synthesized two components to help determine whether the third-party doctrine will apply to private data conveyed to third parties. "First, all information must be voluntarily conveyed to a third party before it loses Fourth Amendment protection. Second, only third-party participants have the authority to consent to disclosure; mere intermediaries do not."[206] The conditions under which data is transmitted to third parties sheds light on the voluntariness and extent of sharing.

The first area of inquiry in third-party doctrine scenarios looks at the "voluntariness" of conveying the data to the third party. Of course, individuals who spit in a tube and provide their DNA to genealogy companies such as 23andMe or Ancestry, are voluntarily providing these companies with DNA samples. As discussed earlier, these samples are chock full of intimate information: data about one's heritage, close and distant relatives, Neanderthal connections, genetic mutations, genetic predispositions to certain diseases and other medical information. This information could be used to predict life expectancy, future health care costs, and (science fiction aside) the necessary material to perhaps one day make an exact replica clone.[207] Spinoff genealogy sites, such as GEDmatch, do not accept and test DNA samples from their users, instead allowing users to voluntarily upload (for free) the raw results of their DNA testing from companies such as Ancestry and 23andMe.[208]

In addition to DNA samples, genealogy sites also collect other critical personal data from users. For example, during registration GEDmatch gathers the user's "name, an optional alias, and email address."[209] Once registered, the user provides the site other personal information such as "sex, Y-DNA or mtDNA haplogroup, genetic sequence/information, Genealogy data, and/or Tier 1 payment information."[210] Further, users may "engage in forums that are designed to be visible to other users, including comments and postings."[211] Ancestry and 23andMe have similar policies.[212]

Genealogy websites usually have policies to ensure that the uploaded DNA samples and other sensitive private information are provided by the owner

---

206 Ormerod & Trautman, *supra* note 20, at 145.

207 *See also* Suter, *supra* note 122, at 739. Professor Suter contends it "is difficult to know with respect to any individual which pieces of their genetic information will be sufficiently distinct from others or informative with respect to susceptibility to disease, temperament, and other traits." *Id.* at 778.

208 *See, e.g.*, *GEDmatch.Com Terms of Service and Privacy Policy*, *supra* note 86.

209 *Id.*

210 *Id.*

211 *Id.*

212 *See Ancestry Terms and Conditions*, *supra* note 156; *Privacy Statement*, 23ANDME, https://www.23andme.com/about/privacy/ (last updated Aug. 22, 2019).

(or authorized user) of the data.[213] GEDmatch manages this issue by requiring those who upload their raw DNA data to make certain representations to the website owners:[214] that it is either their own DNA or else that they are authorized to upload it.[215] If a user does not have specific permission to reveal other genealogy data, the user agrees "to privatize living individuals in your Genealogy Data prior to providing it to GEDmatch" by "changing the names of living individuals to 'LIVING' or something similar," or else face the penalty of having the user's data deleted.[216]

The second area of inquiry in third-party doctrine scenarios is to determine whether the person releasing the sensitive DNA data is a "third-party participant" (and not a "mere intermediary").[217] Most genealogy sites have privacy terms to inform their users about the privacy that protects their uploaded sensitive data.[218] For example, Ancestry explains it "does not share your individual Personal Information (including your Genetic Information) with third-parties without your additional consent . . . . [W]e will not share your Genetic Information with insurance companies, employers, or third-party marketers without your express consent."[219] GEDmatch states that "all Genealogy Data provided to GEDmatch can be viewed, searched, and compared

---

[213] *See, e.g.*, *Ancestry Terms and Conditions*, *supra* note 156; *Privacy Statement*, *supra* note 212; *GEDmatch.Com Terms of Service and Privacy Policy*, *supra* note 86.

[214] *GEDmatch.Com Terms of Service and Privacy Policy*, *supra* note 86. The user represents that it is their own DNA or else the

> DNA of a person for whom you are a legal guardian; DNA of a person who has granted you specific authorization to upload their DNA to GEDmatch; DNA of a person known by you to be deceased; DNA obtained and authorized by law enforcement to identify a perpetrator of a violent crime against another individual, where 'violent crime' is defined as murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault; DNA obtained and authorized by law enforcement to identify remains of a deceased individual; [a]n artificial DNA kit (if and only if: (1) it is intended for research purposes; and (2) it is not used to identify anyone in the GEDmatch database); or DNA obtained from an artifact (if and only if: (1) you have a reasonable belief that the Raw Data is DNA from a previous owner or user of the artifact rather than from a living individual; and (2) that previous owner or user of the artifact is known to you to be deceased).

Id.

[215] *Id.*

[216] *Id.* The penalty for violating GEDmatch's policy is to "have their Raw Data or other personal information deleted without warning, their access will be blocked, and/or other remedial steps may be taken, including any legal action allowed under law." *Id.*

[217] *See* Ormerod & Trautman, *supra* note 20, at 145.

[218] *See, e.g.*, *GEDmatch.Com Terms of Service and Privacy Policy*, *supra* note 86; *Privacy Statement*, *supra* note 212.

[219] *See, e.g.*, *Your Privacy*, ANCESTRY (July 25, 2019), https://www.ancestry.com/cs/legal/privacystatement (emphasis omitted).

by any GEDmatch user," but users can partly protect their privacy by "providing an alias for either login or data."[220]

Most genealogy websites also allow their users to choose the level of privacy over their data. Even GEDmatch[221]—used extensively by law enforcement before and after the Golden State Killer breakthrough—updated its policies in May 2019 to increase the privacy rights of its customers. Under its revised terms of service, GEDmatch allows users to designate their data "private," meaning it "is not available for comparisons with other people. It may be usable in some utilities that do not depend on comparisons with other DNA."[222] Data that a user designates as "public + opt-in" is "available for comparison to any Raw Data in the GEDmatch database using the various tools provided for that purpose."[223] Data that a user designates as "public + opt-out" is

> available for comparison to any Raw Data in the GEDmatch database, except DNA kits identified as being uploaded for Law Enforcement purposes. Comparison results, including your kit number, name (or alias), and email will be displayed for "Public" kits that share DNA with the kit being used to make the comparison, except that kits identified as being uploaded for Law Enforcement purposes will only be matched with kits that have "opted-in."[224]

Finally, data designated "research" is "available for one-to-one comparison to other Public or Research DNA. It is not shown in other people's 'one-to-many' results lists. The Raw Data that you uploaded is not made available."[225]

Also, recall from Part III that genealogy sites recognize that the DNA samples, test results, and other private data uploaded to these sites generally are the property of the user. For example, Ancestry users "always maintain ownership of [their] data,"[226] and GEDmatch affirms that "[r]aw DNA data

---

220 *See, e.g.*, *GEDmatch.Com Terms of Service and Privacy Policy*, *supra* note 86. The website warns that "any personally identifiable information you choose to submit via [its] forums can be read, collected, and used by other participants and could be used to send you unsolicited messages." *Id.*

221 *Id.* Law enforcement officials are concerned about the ongoing viability of GEDmatch under its revised policy. *See* Kristen V. Brown, *DNA Site that Helps Cold-Case Sleuths Curbs Access for Cops*, BLOOMBERG (June 10, 2019, 10:00 AM), https://www.bloomberg.com/news/articles/2019-06-10/dna-site-that-helps-cold-case-sleuths-curbs-access-for-police (quoting a Parabon genealogist that GEDmatch is "basically useless now" to the police and the company's "work on any new cases is significantly stalled").

222 *GEDmatch.Com Terms of Service and Privacy Policy*, *supra* note 86.

223 *See, e.g.*, *id.*

224 *Id.*

225 *Id.*

226 *See, e.g.*, *Ancestry Terms and Conditions*, *supra* note 156.

uploaded to GEDmatch.Com ('Raw Data') remains the property of the person who uploaded it."[227] With the fact of property ownership comes the right to exclude others from the data. Thus, in addition to privacy settings, some companies give the user control over what information is maintained on the website. For instance, 23andMe gives its users the ability to share information by choosing whether to "store or discard your saliva sample after it has been analyzed"; which "health report(s) you view and/or opt-in to view"; "[w]hen and with whom you share your information, including friends, family members, health care professionals, or other individuals outside our Services, including through third-party services that accept 23andMe data and social networks;" and to "give or decline consent for 23andMe Research;" and to "delete your 23andMe account and data, at any time."[228] And GEDmatch allows users to delete family trees and other genealogy data simply by "clicking on the 'Manage your resources' link on your home page."[229]

2. Data-Sharing with Law Enforcement on Genealogy Websites

In the context of police searches of genealogy sites, one other category of information is critical—the level of informed consent each genealogy site provides its users about how their private information will (or will not) be shared with law enforcement. This is particularly important to help determine whether users waive any privacy objections by expressly authorizing the sharing of their information with the police. If so, these would not be PAL Level 3 or 4 scenarios but Level 5, where express consent has defeated any potential privacy rights sought to be vindicated. Here, the private sites (i.e., Ancestry and 23andMe) have taken a different approach than some of the publicly available websites (i.e., GEDmatch), with the private sites expressly resisting law enforcement cooperation and GEDmatch being more cooperative.

Ancestry and 23andMe notify their users that they will fully resist law enforcement within the bounds of the law. Ancestry's published guidance for law enforcement data requests contains the following information policies:

> Ancestry will release basic subscriber information as defined in 18 USC § 2703(c)(2) about Ancestry users to law enforcement only in response to a valid trial, grand jury or administrative subpoena. Ancestry will release additional account information or transactional information pertaining to an account (such as search terms, but not including the contents of communications) only in response to a court order issued pursuant to 18 USC §

---

227 *See, e.g.*, *GEDmatch.Com Terms of Service and Privacy Policy*, *supra* note 86.

228 *See, e.g.*, *Privacy Statement*, *supra* note 212.

229 *See, e.g.*, *GEDmatch.Com Terms of Service and Privacy Policy*, *supra* note 86. The site provides a "link or other means . . . to remove your Raw Data from the Site. Alternatively, you can request deletion of your personal information at any time by contacting us." *Id.*

> 2703(d). Contents of communications and any data relating to the DNA of an Ancestry user will be released only pursuant to a valid search warrant from a government agency with proper jurisdiction. If we receive a valid request under U.S. law to preserve records that constitute potentially relevant evidence in legal proceedings, we will preserve, but not disclose, a temporary snapshot of the relevant account records for 90 days pending service of valid legal process as described above.[230]

When records are demanded via a proper warrant, Ancestry will "notify users of the request and provide a copy of the request prior to disclosure, unless [it is] legally restricted from doing so" by a "court order pursuant to 18 U.S.C. § 2705(b) or equivalent state statute that is signed by a judge."[231] Significantly, Ancestry also provides the possibility of releasing information to law enforcement in "an exigent emergency that involves the danger of death or serious physical injury to a person that Ancestry may have information necessary to prevent," if law enforcement sends an "emergency disclosure request" including the identity of the person in danger; the "nature of the emergency (e.g., report of suicide, bomb threat)"; the account holder's "username and the email and/or mailing address"; the "specific information requested and why that information is necessary to prevent the emergency"; and all other "details or context."[232] 23andMe has similarly strict policies that seek to avoid cooperation with law enforcement in most cases.[233]

---

[230] *Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/cs/legal/lawenforcement (last visited Aug. 28, 2019).

[231] *Id.*

[232] *Id.*

[233] 23andMe also reports any requests to users, when possible, and has this to say about its philosophy toward providing data to law enforcement:

> 23andMe chooses to use all practical legal and administrative resources to resist requests from law enforcement, and we do not share customer data with any public databases, or with entities that may increase the risk of law enforcement access. In certain circumstances, however, 23andMe may be required by law to comply with a valid court order, subpoena, or search warrant for genetic or personal information.
>
> 23andMe requires valid legal process in order to consider producing information about our users. 23andMe will only review inquiries as defined in 18 USC § 2703(c)(2) related to a valid trial, grand jury or administrative subpoena, warrant, or order. . . . 23andMe will consider releasing additional account information or transactional information pertaining to an account only in response to a court order issued pursuant to 18 USC § 2703(d). In addition, 23andMe will only consider inquiries from a government agency with proper jurisdiction.
>
> If a 23andMe user completes a valid authorization to disclose their Genetic Information to law enforcement, then 23andMe will disclose the information identified in the authorization. 23andMe will not disclose any identifying information about the authorizing user's genetic relatives or connections that 23andMe holds unless those users also provide express, written consent.

But requests of this type appear to be infrequent as of early 2019. For instance, Ancestry reported to the Associated Press (AP) that it had not "received such requests for genetic information in the last three years," and 23andMe informed the AP that it had "'never given customer information to law enforcement officials'" despite five requests from law enforcement about Americans' data.[234] In 2018, Ancestry reported it had received ten law enforcement requests for user information; it had "provided information in response to 7 of those 10 requests"; all requests were related to "investigations involving credit card misuse and identity theft"; it had "refused numerous inquiries on the basis that the requestor failed to obtain the appropriate legal process"; and it had "received no valid requests for information related to genetic information of any Ancestry member, and we did not disclose any such information to law enforcement."[235]

In contrast, GEDmatch has made a conscious decision to cooperate with law enforcement, but only in certain types of serious crime investigations. First, the site warns its users that the sensitive private data they provide to GEDmatch can be used for "[f]amilial searching by third parties such as law enforcement agencies to identify the perpetrator of a crime, or to identify remains."[236] It also informs users that it "may disclose your Raw Data, personal information, and/or Genealogy Data if it is necessary to comply with a legal obligation such as a subpoena or warrant. We will attempt to alert you to this disclosure of your Raw Data, personal information, and/or Genealogy Data, unless notification is prohibited under law."[237]

After the Golden State Killer case became public, GEDmatch made a policy decision to provide additional informed consent to its users to get their permission to allow those types of intrusions by the government, and it tightened the terms of that policy in May 2019. Its revised terms of service authorize (police) users to load "DNA obtained and authorized by law enforcement to identify a perpetrator of a violent crime against another individual, where 'violent crime' is defined as murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault; [and] DNA obtained and authorized by law enforcement to identify remains of a deceased individual"—although this data will now only be compared to the data of those customers who expressly "opt-

---

23andMe Guide for Law Enforcement, 23ANDME, https://www.23andme.com/law-enforcement-guide/ (last visited Aug. 28, 2019).

234 Fiza Pirani, *Can Police Legally Obtain Your DNA from 23andMe, Ancestry?*, ATLANTA J.-CONST. (May 11, 2018), https://www.ajc.com/news/national/can-police-legally-obtain-your-dna-from-23andme-ancestry/8eZ24WN7VisoQiHAFbcmjP/. *See, e.g., 23andMe Guide for Law Enforcement*, *supra* note 233.

235 *Ancestry 2018 Transparency Report*, ANCESTRY, https://www.ancestry.com/cs/transparency (last visited Aug. 28, 2019).

236 *See, e.g., GEDmatch.Com Terms of Service and Privacy Policy*, *supra* note 86.

237 *Id.*

in" to such comparisons.[238] This was the technique the police used in the Golden State Killer case—creating a false profile with the unknown DNA evidence and loading it up to GEDmatch in search of relatives and then creating a family tree.

3. Applying the Third-Party Doctrine after *Carpenter*

In light of the genealogy sites' privacy policies and informed consent regarding cooperation with (or resistance to) law enforcement, the final question to consider is whether, after *Carpenter*, the third-party doctrine should be applied to negate Fourth Amendment privacy interests possessed by individuals in their own DNA and test results (i.e., PAL Levels 3 or 4). This section will address each of those scenarios in turn.

Before diving in, consider the analysis prior to the Supreme Court's decision in *Carpenter v. United States.* Prior to that case, the typical third-party analysis would have first noted that users have provided their own personal DNA data "voluntarily" to a third party and that it is the actual "third-party participants" (i.e., the genealogy companies) that are distributing the users' DNA data to the police.[239] This would weigh in favor of applying the third-party doctrine. Then, the analysis would have observed that users of genealogy sites "assumed the risk" when they gave their sensitive private data to a third party, taking the chance that the genealogy companies might "betray" them by giving that private data to the police to search. For some, that might be the end of the analysis because any "reasonable" expectation of privacy under *Katz* became unreasonable once the user assumed the risk of entrusting their data to a third party.

But it is worth pausing a moment to recognize that, even in a pre-*Carpenter* world, the Supreme Court had drawn a distinction between "non-content" information (e.g., telephone numbers, addresses) and "content" data (e.g., substance of phone conversations, content of letters).[240] Indeed, Justice Kennedy's dissent in *Carpenter*—while defending the third-party doctrine on its face—acknowledged that the doctrine had traditionally accepted limits: it "may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party."[241] Of course, some "content" disclosures are traditionally covered by the third-party doctrine, such as the bank papers in *Miller*. But that is because those documents "were 'negotiable instruments' that were 'to be used in commercial transactions.' The third-party doctrine thus recognizes two

---

238 *Id.*

239 Ormerod & Trautman, *supra* note 20, at 145.

240 *See* Wilson, *supra* note 186, at 17.

241 Carpenter v. United States, 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting) (citing Ex parte Jackson, 96 U.S. 727, 733 (1878) (letters held by mail carrier); United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2010) (e-mails held by Internet service provider)).

distinctions—one between content and non-content and one between personal communications and business records."[242]

With that caveat, one might have argued, even before *Carpenter*, that giving up the content of one's DNA test is more like the substance of a letter ("content") than mere addressing information ("non-content"). Also, a DNA test result is not the kind of commercial "business record" held by a bank as part of a negotiable-instruments framework, but more like a personal communication (perhaps a biological diary). And, before *Carpenter*, the analysis likely would have led to a discussion of *Maryland v. King*'s distinction that searching "junk DNA" for mere identification information is more like recording telephone numbers than the substance of a telephone call (assuming the police only use the junk DNA for its identification purposes).[243] More on that below.

Enter *Carpenter*. Recall that the *Carpenter* Court articulated two reasons not to extend the third-party doctrine to the collection of CSLI: (1) the primary rationale for the third-party doctrine (that only limited information can be gleaned from data such as telephone numbers) did not apply due to the nature of CSLI, which made it possible to track everyone's location for years;[244] and, (2) the assumption-of-risk rationale did not apply because CSLI "is not truly 'shared' as one normally understands the term" due to the "indispensable" requirement to carry a cell phone for "participation in modern society" and because cell phones log location data "without any affirmative act on the part of the user beyond powering up," thus defeating the notion the user "assumed the risk" in any "meaningful sense."[245] Each of these rationales will be applied below in the DNA context.

First, are DNA and test-result data more like CSLI or more like telephone numbers and business records, the items to which the third-party doctrine was intended to apply? For the reasons discussed in Parts II and III, DNA information is more like CSLI, given its ability to store immense amounts of intimate data. But this leads back to the Court's analysis in *King*, which has been accepted by lower courts as the proper distinction when the government uses CODIS to search "junk DNA" (with no known coding functions) for the *sole* purpose of identifying a person.[246] Recall, however, that private genealogy companies go beyond the purposes and techniques used in CODIS to merely identify suspects. These services also look deep into heritage, health, and research. Further, genealogy searches work differently than CODIS, as Ancestry explained when discussing its "autosomal DNA test," which surveys "a person's

---

242 Ormerod & Trautman, *supra* note 20, at 117–18.

243 *See* Maryland v. King, 569 U.S. 435, 464 (2013) (reasoning that "CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee" and are not tested for that purpose).

244 *Carpenter*, 138 S. Ct. at 2219–20.

245 *Id.* at 2220.

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

entire genome at over 700,000 locations."[247] Thus, it seems fair to say—assuming the police truly are seeking the *contents* of a DNA test result contained on a genealogy site—that this presents a distinguishable situation from *King*. If the police seek "content data" within DNA or in test results generated by a genealogy company, then the first rationale for the third-party doctrine seems inapplicable, as in *Carpenter*.

But one might still want to argue as in *King* that, even considering the additional data in genealogy databases, the police are not interested in any of that data and merely want to find a suspect's relatives for identification purposes. Thus, perhaps this search is exactly like *King*, even though it takes place outside of CODIS. But even if it were true that the police did not seek this additional data, the problem with that position is it minimizes *King's* reliance on the search occurring in the "junk" portion of DNA, and also that the government sincerely could argue CODIS existed only for identification purposes. With private databases, neither of those conditions is true. Searches used by private databases go beyond junk DNA, and the databases themselves exist for many more functions in addition to identification. *King* is entirely distinguishable.

The second inquiry asks whether the assumption-of-risk rationale applies to DNA data, or whether that rationale falls away as it did in *Carpenter* because CSLI was not "voluntarily" given. Here, the argument in favor of *applying* the third-party doctrine is stronger than in *Carpenter*. Unlike CSLI, there is nothing "indispensable" to modern society in giving one's DNA data to a genealogy company. One might argue that the genealogy boom has made it so that everyone does and should want to know their heritage and the identity of their biological relatives, but this still seems a far distance removed from the cell-phone situation. (Perhaps one day the DNA issue will permeate as thoroughly as cell phones, but that remains to be seen.)

Also, unlike with CSLI, users take several deliberate "affirmative acts" before their private data is placed in the hands of a third party. This is not a situation where one's DNA is automatically uploaded to a database when one "powers up," as with CSLI. Indeed, based on the privacy policies described earlier, users have full control over their data. Not only do they choose to spit in a tube and mail it to 23andMe, they also choose to upload those results on websites, to upload additional personal information, to make their data searchable by other users, and to delete (or keep) their data on the website. Everything about the process is deliberate, including the reading and acknowledging of terms of service and privacy statements.

Thus, under the second rationale discussed in *Carpenter*, a much stronger argument can be made that DNA users have "assumed the risk" that a third party would betray them and open their data to a police search, regardless of what the privacy policies say. Recall that those policies were premised on the understanding that law enforcement could access DNA data with an

---

[247] *AncestryDNA - Frequently Asked Questions*, *supra* note 83.

administrative warrant of the type authorized by the Stored Communications Act, which uses a standard less than Fourth Amendment probable cause. Unlike CSLI data, the DNA data turned over to genealogy websites appears more suited to the traditional assumption-of-risk analysis that is central to the third-party doctrine.

Perhaps this analysis justifies applying the third-party doctrine in Level 3 scenarios, despite Ancestry and 23andMe's insistence that they will not turn over one's data to the police. And surely this analysis justifies applying the third-party doctrine in Level 4 scenarios, where companies such as GEDmatch have openly stated they will share the information with law enforcement for familial searching purposes and that they have authorized the police to load up DNA samples on their site to help solve serious crimes. That is a classic assumption-of-risk scenario.

But before concluding that the third-party doctrine will defeat whatever potential Fourth Amendment privacy interest was recognized above in Part III, one other item must be discussed. Recall that the third-party doctrine was designed to deal with the modern *Katz* approach to "reasonable expectations of privacy." Would the doctrine similarly defeat a traditional property-based approach, as Justice Gorsuch articulated in his dissent in *Carpenter*? Or is this a situation where the property-rights approach provides greater privacy protections than *Katz*?

In his dissent in *Carpenter*, Justice Gorsuch argued that

> the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them. Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a bailment.[248]

He contended that a "bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the 'implication[s] from their conduct' if they don't."[249] He argued that a person may not lose their Fourth Amendment interest in the contents of their data just because they entrust it to a third party: "Whatever may be left of *Smith* and

---

[248] *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting). Gorsuch explained that a bailment is the "delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose." *Id.* at 2268–69 (citing BLACK'S LAW DICTIONARY 169 (10th ed. 2014); J. STORY, COMMENTARIES ON THE LAW OF BAILMENTS § 2, at 2 (1832) ("[A] bailment is a delivery of a thing in trust for some special object or purpose, and upon a contract, expressed or implied, to conform to the object or purpose of the trust.")).

[249] *Carpenter*, 138 S. Ct. at 2268–69 (Gorsuch, J., dissenting) (citing 8 C.J.S. *Bailments* § 36, at 468–69 (2017)).

Miller, few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest."[250]

In the Level 3 scenario with Ancestry and 23andMe, considering the types of contracts into which users enter (including the companies' law-enforcement-resistant provisions), and in light of the very real property interest that a person has in one's own DNA and test results, it would seem Justice Gorsuch's property-based approach would permit Fourth Amendment protection. Not only is a protected property interest at stake, but the owner of the property has merely created a bailment with the genealogy companies to hold the DNA data in trust for as long as the owner wishes to keep it with them. A trespass on that data is still a trespass on a current property interest owned by the user, and hence a violation of the Fourth Amendment. Still, a different result is probably reached in the Level 4 scenario with GEDmatch, where the owner of the data has expressly agreed by contract to open up their DNA data to search by law enforcement (unless perhaps the police exceed the bounds of the licensed search in the GEDmatch contract with the user). In that case, the owner has licensed the search.

In sum, considering the Level 3 and 4 scenarios where the DNA owner entrusts data to a third-party genealogy company, any expectation of privacy recognized in a *Katz* analysis likely is extinguished by the third-party doctrine. Although DNA data is immense, as with CSLI, the assumption-of-risk rationale significantly undergirding that doctrine provides a valid basis to apply the doctrine. But, under a traditional property-based approach, the third-party doctrine likely would not defeat the protected property interests in a Level 3 scenario, although a search might still be proper in a Level 4 scenario due to contract licensing terms. In either event, because Part III concluded one does not have a protected Fourth Amendment interest in the DNA or test results of a biological relative, nothing in that Amendment would prevent police from searching the DNA results of a criminal subject's biological relatives to find an identity match.

V. FUTURE ALTERNATIVES TO PROTECT GENETIC PRIVACY AFTER *CARPENTER*

This Article has identified areas where the Fourth Amendment does and does not protect an individual's DNA and test results submitted to private genealogy websites. While, after *Carpenter*, there is a plausible chance the U.S. Constitution will sometimes prevent law enforcement from searching those

---

[250] *Id.* at 2269. Gorsuch also doubted that "complete ownership or exclusive control of property is always a necessary condition" under the Fourth Amendment because, "[w]here houses are concerned, for example, individuals can enjoy Fourth Amendment protection without fee simple title. Both the text of the Amendment and the common law rule support that conclusion." *Id.*

databases without probable cause, it is likely that any protection would not extend beyond an individual's right to protect their own test results from unlawful search. So what protections exist to regulate police familial searches of the DNA results of biological relatives? In Part V, this Article briefly comments on the current state of the law and the need for further protections. It then offers some preliminary thoughts to be pursued in future articles on potential legislative solutions to protect individual privacy in this area.

A. The Need for Protection

The lightning-paced evolution of DNA technology has led to greater and sooner advances in DNA research than previously expected. Even as NDIS and other law enforcement DNA databases expand, advances in technology make future DNA testing cheaper and more accessible. The advent of "touch DNA" now allows law enforcement to "obtain full forensic DNA profiles from exceedingly small amounts of biological material" such as "skin cells shed when touching objects" like "the handle of a gun, the portion of a torn screen touched by an intruder, a brick used to break a window in a burglary, or the steering wheel of a stolen vehicle."[251] The use of Rapid DNA analysis has also opened the possibility for local DNA processing without resort to crime labs.[252]

And the capability to exploit these DNA databases is growing daily. Researchers in October 2018 concluded that police could use private genealogy databases to identify crime suspects with increasing accuracy, and that "about 60% of the searches for individuals of European-descent will result in a third cousin or closer match[.]"[253] In a different study released the same month, researchers concluded that an individual's DNA (or the DNA of a relative) contained in certain genealogy databases could be identified by linking that data "to a CODIS profile, and vice versa, in a manner not intended in the context of either database examined in isolation," which "could expose relatives of the

---

[251] Kreag, *supra* note 72, at 1504.

[252] *Id.* (noting the development of "a stand-alone, fully-automated DNA processing machine that can process a biological sample and obtain a forensic DNA profile in ninety minutes").

[253] Yaniv Erlich et al., *Identity Inference of Genomic Data Using Long-Range Familial Searches*, SCIENCE (Oct. 11, 2018), http://science.sciencemag.org/content/early/2018/10/10/science.aau4832 (study led by chief science officer at the genealogy company, MyHeritage, using "genomic data of 1.28 million individuals tested with consumer genomics"); *see also* Rob Stein, *Easy DNA Identifications with Genealogy Databases Raise Privacy Concerns*, NAT'L PUB. RADIO (Oct. 11, 2018, 3:58 PM), https://www.npr.org/sections/health-shots/2018/10/11/656268742/easy-dna-identifications-with-genealogy-databases-raise-privacy-concerns (quoting Erlich as saying that "each person in this database is a beacon that illuminates hundreds of distant relatives. So it's enough to have your third cousin or your second cousin once-removed in these databases to actually identify you.").

participant to forensic investigation; moreover, phenotypes of a relative could potentially be identifiable from a forensic profile."[254]

As these capabilities grow, the potential for indiscriminate and unchecked police use of private DNA databases to identify criminals should be a concern for those who care about privacy. As Justice Scalia warned in *King*, the government could solve more crimes by taking DNA from "anyone who flies on an airplane . . . , applies for a driver's license, or attends a public school. Perhaps the construction of such a genetic panopticon is wise. But I doubt [our Founders] would have been so eager to open their mouths for royal inspection."[255] Yet that is exactly what millions of Americans have done voluntarily—opened their mouths for inspection and for cataloguing in a private database, perhaps unaware that the government could exploit that act for solving crime.

Some scholars have argued that police DNA searches, especially familial searches, "should be forbidden because they embody the very presumptions that our constitutional and evidentiary rules have long endeavored to counteract: guilt by association, racial discrimination, propensity, and even biological determinism."[256] They worry about the impact of these searches on innocent relatives of suspects, on unfairly targeted racial minorities,[257] and on those whose privacy will be invaded by the inevitable inaccuracies in testing DNA samples recovered from a crime scene.[258] As this Article noted in its introduction, even the Golden State Killer investigation first swabbed two false leads before finding a true match. What impact does that have on the life of the person who has fallen under a cloud of suspicion for some period of time?

Legislatures have taken some action in the past decade to deal with issues related to DNA testing and research. And though some states have passed laws that "prohibit genetic discrimination by health insurers and employers," those laws often include exceptions for law enforcement purposes, and none

---

254 Jaehee Kim et al., *Statistical Detection of Relatives Typed with Disjoint Forensic and Biomedical Loci*, 175 CELL 848, 848–49 (Oct. 18, 2018), https://www.cell.com/cell/pdf/S0092-8674(18)31180-2.pdf; *see also* Stein, *supra* note 253 (discussing the study).

255 Maryland v. King, 569 U.S. 435, 482 (2013) (Scalia, J., dissenting).

256 Murphy, *supra* note 57, at 304.

257 *Va. to Use Familial DNA in Criminal Investigations*, DENVER POST (Mar. 21, 2011), https://www.denverpost.com/2011/03/21/va-to-use-familial-dna-in-criminal-investigations/ (discussing Maryland's decision in 2008 to ban familial searches using its DNA database because it would have put half the state's African-American population under possible surveillance because of the disproportionate number of black men who are subject to arrest).

258 *See* Erin Murphy, *The Art in the Science of DNA: A Layperson's Guide to the Subjectivity Inherent in Forensic DNA Typing*, 58 EMORY L.J. 489, 497 (2008); *see also* Strutin, *supra* note 6, at 347 (explaining that "every stage in the collection, profiling, databanking and analysis of DNA evidence can be subject to human error, mechanical error, computer error, statistical error, false positives and cognitive biases").

provide protections regarding familial searching.[259] Following the lead of scholars and scientists, some legislatures have considered bills modeled on the Genetic Privacy Act proposed by a group of bioethicists,[260] and state and federal governments have started to provide protection in the employment discrimination context.[261] But none of those laws address the privacy concerns raised by law enforcement searches of genealogy databases.[262]

Nor do current privacy-based laws—such as wiretapping statutes, the Stored Communications Act, or HIPAA—provide answers to this problem. Professor Natalie Ram summarizes the current lack of regulation in this area:

> In other contexts, Congress has acted to create statutory protections, so we have the Stored Communications Act, which gives certain privacy protections for your emails. But we don't have any sort of analogous law for ordinary genetic data like the genealogical data at issue in the Golden State Killer investigation. We do have protections in some other settings: so your identifiable health information might be protected under the HIPAA Privacy Rule, and certain kinds of data used for research purposes can be eligible for other kinds of protections. But generally speaking, your genetic information in a commercial, direct-to-consumer website setting, there isn't a lot of legal protection that's obviously available.[263]

More must be done.

---

259 Gabel, *supra* note 58, at 30–31.

260 GEORGE J. ANNAS ET AL., THE GENETIC PRIVACY ACT AND COMMENTARY (1995), https://web.ornl.gov/sci/techresources/Human_Genome/resource/privacyact.pdf.

261 *See* Genetic Information Nondiscrimination Act of 2008, 42 U.S.C.A. § 2000ff (West 2019), which took effect November 21, 2009. State genetic discrimination laws include MASS. GEN. LAWS ANN. ch. 111, § 70G(c) (West 2019); MICH. COMP. LAWS ANN. §§ 333.17020, 17520 (West 2019); NEB. REV. STAT. ANN. § 71-551 (West 2019); and OR. REV. STAT. ANN. § 192.53 (West 2019).

262 For instance, the Genetic Privacy Act ensures that nothing "shall be construed to prohibit federal, state or local law enforcement authorities from collecting, storing or typing DNA samples" as authorized by law for the "limited . . . purpose of matching DNA samples in criminal investigations," with restricted access to "authorized law enforcement agencies, prosecutors, defense counsel, defendants, accused individuals, suspects, and their authorized agents." ANNAS ET AL., *supra* note 260, at § 122.

263 Mina Kim, *Are Family Tree Sites Fair Game for Law Enforcement?*, WBUR (May 2, 2018, 8:39 AM), http://www.wbur.org/hereandnow/2018/05/01/golden-state-killer-family-tree-sites; *see also* Ford, *supra* note 15 (relating Professor Suter's position that patient privacy rules do not automatically apply to "genealogy databases—even the ones that use submitted DNA samples to check for potential genetic illnesses").

B. Potential Legislative Considerations

In Parts III and IV, this Article provided an argument in support of some Fourth Amendment protections for suspects with regard to law enforcement access to their DNA test results, even those held by third-party genealogy companies and found on publicly accessible websites. But while there may be an argument in favor of that protection, there is little chance the Fourth amendment protects a criminal subject from the police search of DNA data belonging to that subject's biological relatives. Yet there are compelling reasons for Congress and state legislatures to act to curb the potential for unfettered police practices. And, as with so many other policy issues, it should not be the role of the courts to make policy and constitutionalize the area of DNA testing when state and federal legislators are more than capable of addressing the problem.

In *United States v. Jones*, Justice Alito commented on the need and desirability for legislative intervention to provide democratic protections against police overreach in the digital age. Noting the "concern about new intrusions on privacy," Justice Alito expressed the hope this might "spur the enactment of legislation to protect against these intrusions."[264] He compared the situation to that of wiretapping after *Katz*, where "Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute . . . and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law."[265] His comments echoed the Court's thoughts a few years earlier, in *District Attorney's Office for the Third Judicial District v. Osborne*,[266] where it refused to apply the Due Process Clause to create a new substantive right of a convicted person to access a state's DNA evidence, explaining:

> DNA evidence will undoubtedly lead to changes in the criminal justice system. It has done so already. The question is whether further change will primarily be made by legislative revision and judicial interpretation of the existing system, or whether the Federal Judiciary must leap ahead—revising (or even discarding) the system by creating a new constitutional right and taking over responsibility for refining it.[267]

---

264 United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

265 *Id.*

266 557 U.S. 52 (2009).

267 *Id.* at 74. The Court expounded on its concern about the need for refinement:

> The first DNA testing statutes were passed in 1994 and 1997. In the past decade, 44 States and the Federal Government have followed suit, reflecting the increased availability of DNA testing. . . . If we extended substantive due process to this area, we would cast these statutes into constitutional doubt and be forced to take over the issue of DNA access ourselves. We are reluctant to enlist the Federal Judiciary in creating a new constitutional code of rules for

Professor Murphy, in proposing a three-fold goal of closely regulating familial searches (i.e., "to minimize their intrusiveness, optimize their efficacy, and ensure their legality"), has recommended regulations over when such searches could occur, the technical parameters delimiting the scope of the searches, the databases subject to search, regulations following a potential familial match, and creation of structural oversight of the process.[268] And Professor Jessica Gabel has proposed language for a statute involving familial DNA searching.[269]

In the future, these and other proposals should be built upon to develop legislation that could provide a balanced approach to preserving privacy rights while not handicapping legitimate law enforcement efforts in this area.

VI. CONCLUSION

The Fourth Amendment has evolved with the times, especially as new and unexpected technologies have revolutionized both crime and law enforcement techniques. This Article has explored the issue of warrantless police searches of private genealogy databases after *Carpenter v. United States*, focusing on whether the Fourth Amendment protects DNA test results—both a person's own results and those of their biological relatives—and whether the third-party doctrine is viable in that context. It traced the roots of the Supreme Court's property-based and modern *Katz* "reasonable expectation of privacy" approaches to the Fourth Amendment and described the development of the third-party doctrine. Examining the *Carpenter* decision, it analyzed the Court's modified approach—including its new multifactor balancing test—and the two rationales it employed in limiting the third-party doctrine with regard to cell-site location information (CSLI).

Then, in light of *Carpenter*—and using both the traditional property-based and modern *Katz* approaches—it analyzed whether the Fourth Amendment would protect a criminal subject's DNA data from the police search of a private genealogy database. It concluded that a plausible argument supports such protection under both approaches. But it also found a strong basis to reject any Fourth Amendment claim of a criminal subject in the DNA data of a biological relative. Next, exploring the third-party doctrine, it found that doctrine likely to defeat a claim of privacy under the *Katz* approach because the

---

> handling DNA. Establishing a freestanding right to access DNA evidence for testing would force us to act as policymakers, and our substantive-due-process rulemaking authority would not only have to cover the right of access but a myriad of other issues. We would soon have to decide if there is a constitutional obligation to preserve forensic evidence that might later be tested. . . . No doubt there would be a miscellany of other minor directives.

Id. at 73–74 (citations omitted).

268 Murphy, *supra* note 57, at 340–47.

269 Gabel, *supra* note 58, at 53–56.

assumption-of-risk rationale would apply. Yet the property-based approach discussed by Justice Neil Gorsuch in his *Carpenter* dissent might still offer protection under a bailment theory, despite the involvement of a third party. Finally, it briefly set forth the need for legislative action to prevent unfettered police action in this area, and suggested areas for future research.

With technology continuing to advance—and the genealogy boom driving millions of consumers to entrust to third parties their DNA and all of its intimate biological secrets—the Fourth Amendment should place some limits on police action in this area. The Court's traditional property-based approach to that Amendment provides the best avenue for those limits. And where the Fourth Amendment's protection ends, legislative action should begin in order to avoid continued invasions of privacy into one of the most sensitive storehouses of intimate data: the human genome itself.