2020

From the Legal Literature: The Threat and Promise of Police Use of DNA Databases

Francesca Laguardia

From the Legal Literature
The Threat and Promise of Police Use of DNA Databases

Francesca Laguardia, J.D., Ph.D.

I. Introduction

According to an op-ed published in *Time* magazine, genealogy is "the second most popular hobby in the U.S. after gardening," with the popularity of online genealogy sites second only to those devoted to pornography.[1] This popularity has led to huge databases of genetic information in the hands of commercial services such as 23 and Me, Ancestry.com, and GEDmatch, with the first two companies alone holding more than 10 million DNA samples.[2] While GEDmatch holds only a million samples, it is an open source (free) database that offers far less privacy protection than do the major commercial databases.[3]

The data held in these records is overwhelming and access to much of that data is, so far, "wholly unregulated."[4] It is a vast trove of searchable information for law enforcement that, thus far, may be accessed without the requirement of a warrant. Law enforcement has been energetically pursuing the opportunities these data present.[5] In the spring of 2018, one such database was used to identify Joseph DeAngelo as the Golden State Killer, a serial killer

---

[1]Antony Kolene, *"23 and Plea": Limiting Police Use of Genealogy Sites After* Carpenter v. United States, 122 W. Va. L. Rev. 53, 65 (2019) (quoting 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/).

[2]Rodriguez, *supra* note 1, at 65.

[3]George M. Dery, III, *Can a Distant Relative Allow the Government Access to Your DNA?*, 10 Hastings Sci. & Tech. L.J. 103, 112–13 (2019).

[4]Sarah Zhang, *How a Genealogy Website Led to the Alleged Golden State Killer*, The Atlantic (April 27, 2018) https://www.theatlantic.com/science/archive/2018/04/golden-state-killer-east-area-rapist-dna-genealogy/559070/ (quoting N.Y.U. School of Law Professor Erin Murphy). Although close familial searches through forensic databases are "highly regulated," searching for distant relatives through open source data is not. *See* Yaniv Erlich, Tal Shor, Itsik Pe'er, & Shai Carmi, *Identity Inference of Genomic Data Using Long-Range Familial Searches* 362 Sci. 690 (2018).

[5]*See*, *e.g.*, Amelia Putnam, *A Genetic Panopticon of Our Own Making: How the Fourth Amendment Applies to Commercial Genealogy DNA Testing*, 56 Crim. L. Bull. 221 (2020).

"believed responsible for 12 killings, 50 rapes, and 100 burglaries from 1974 and 1986."[6] Police made the identification after comparing DNA found at crime scenes to the open source DNA records available on GEDmatch and identifying his distant relatives as relatives of the killer. They found DeAngelo after whittling their options down from a family of over a thousand members to just five possible men.[7] Finally, police obtained DNA from DeAngelo's car door, tested it against the samples they had obtained from crime scenes, and found that his DNA matched.[8]

Since DeAngelo's arrest, law enforcement has used the same techniques to make arrests in over a dozen cases—including the 1992 murder of Christy Mirack and the 1988 rape and murder of eight year old April Tinsley.[9] And in January of this year, police in Chicago announced that they believed they solved a string of murders committed between 1976 and 1981 using genealogical information.[10] In fact, one study found that police used the tactics to make arrests in thirteen cases in just five months, not all of them "cold cases" (that might be considered extreme and justifying extraordinary measures).[11] That same study claimed that 60% of Americans of European descent could be identified by their relatives' use of genealogical databases, and 90% of Americans of European descent would be identifiable within only a few years.[12]

The strength of DNA evidence and the steadily increasing reach of genealogical identification bring fears of an all-seeing, all-knowing, all-powerful government.[13] Can it be possible for the government to

---

[6]Dery, *supra* note 3, at 105.

[7]Dery, *supra* note 3, at 113–14.

[8]Dery, *supra* note 3, at 114.

[9]Dery, *supra* note 3, at 115–16.

[10]David Struett, *Suspected Serial Killer Identified in 1976 Murder of 16-Year-Old Girl in Lisle, Prosecutors Say*, CHI. SUN-TIMES (Jan. 13, 2020), https://chicago.suntimes.com/crime/2020/1/13/21063778/pamela-maurer-bruce-lindahl-lisle-cold-case-murder-strangled-college-road. For more information about the burgeoning field dubbed "forensic genealogy," see Christi J. Guerrini, Jill O. Robinson, Devan Petersen, & Amy L. McGuire, *Should Police Have Access to Genetic Genealogy Databases? Capturing the Golden State Killer and Other Criminals Using a Controversial New Forensic Technique*, PLOS: BIOLOGY (Oct. 2, 2018), https://journals.plos.org/plosbiology/article/file?id=10.1371/journal.pbio.2006906&type=printable.

[11]Erlich et al., *supra* note 4, at 690.

[12]Erlich et al., *supra* note 4, at 690.

[13]*See*, *e.g.*, Zhang, *supra* note 4.

obtain such reach and knowledge without even a warrant? Should the Fourth Amendment allow it?[14]

These questions are hardly new. As technology has improved, more and more technological advancements have triggered privacy fears.[15] Doctrinally, these concerns have been most persistent and developed regarding the ability to track location data provided by portable communication devices (like beepers and cell phones) and GPS devices.[16] In cases raising such concerns, U.S. Supreme Justices began to recognize how developing technology was enabling new levels of privacy violations, by offering insight into intimate aspects of life. For instance, in a single case, Justice Sotomayor expressed her concern that location data provided by a GPS tracking device might reveal details such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church,

---

[14]As Amelia Putnam explained in a previous issue of the Criminal Law Bulletin, the U.S. Department of Justice "announced new guidelines regarding law enforcement's use of genetic genealogy sites for investigative purposes" during the fall of 2019. Putnam, *supra* note 5, at 229 (citing Dep't of Justice, Interim Policy Forensic Genetic Genealogical DNA Analysis and Searching (2019), https://www.justice.gov/olp/page/file/1204386/download).

> The guidelines, which took effect on November 1, 2019, state that genealogy sites can only serve as "an investigative lead" for violent crimes after officers have exhausted all other investigative methods, and a "suspect shall not be arrested based solely on a genetic association generated" by the genealogy results. [But, the] guidelines do not require law enforcement to obtain a search warrant backed by probable cause to conduct the genealogical investigation.

Putnam, supra note 5, at 229.

[15]*See*, *e.g.*, *U.S. v. Knotts*, 460 U.S. 276, 383–84, 103 S. Ct. 1081, 75 L. Ed. 2d 55 (1983) (expressing concern as to whether surveilling an individual by tracking a hidden beeper twenty-four hours a day might create too significant an invasion of privacy for the third party doctrine to negate the violation); *U.S. v. Karo*, 468 U.S. 705, 716–17, 104 S. Ct. 3296, 82 L. Ed. 2d 530 (1984) (holding that although installation of tracking beeper pursuant to an informant's consent did not violate the Fourth Amendment, monitoring it in a private residence violates the homeowner's reasonable expectation of privacy); *Kyllo v. U.S.*, 533 U.S. 27, 34–35, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001) (expressing concern that homeowners' privacy would be left "at the mercy of advancing technology"); *U.S. v. Jones*, 565 U.S. 400, 415, 426, 428, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012) (Justices Alito and Sotomayor's opinions expressing concern as to the extent of privacy invasion achieved through GPS tracking); *Riley v. California*, 573 U.S. 373, 385–86, 134 S. Ct. 2473, 189 L. Ed. 2d 430, 42 Media L. Rep. (BNA) 1925 (2014) (requiring police to obtain a warrant to search the contents of a cell phone); *Carpenter v. U.S.*, 138 S. Ct. 2206, 2220–21, 201 L. Ed. 2d 507 (2018) (finding the use of cell site tracking to surveille defendants to invade on privacy and therefore require a warrant).

[16]*Knotts*, 460 U.S. at 34–35; *Jones*, 565 U.S. at 415–28; *Carpenter*, 138 S. Ct. at 2220–21.

the gay bar and on and on."[17] In that same case, Justice Alito pointed to the ease with which such invasions could be conducted by police departments that at one time "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance. Only an investigation of unusual importance could have justified such an expenditure of law enforcement resources."[18]

Most recently, in *Carpenter v. United States*, the Court held that using cell phone companies' business records to obtain historical location data (cell-site location information) was a search that required a warrant.[19] The Court's ruling was based on an understanding that the Fourth Amendment was intended "to secure 'the privacies of life' against 'arbitrary power' [and] 'to place obstacles in the way of a too permeating police surveillance.' "[20] And while *Carpenter* was, and is, clearly limited to cell phones and cell site location data, any casual observer can see that the threat to which the Court was responding relates to far more varied technology than what has been discussed within the limits of the Court's cases so far. Academics have tried to predict the effects of *Carpenter*, from the use of automated license plate readers[21] and the geolocation and activity data collected by workout apps,[22] to the vast amount of routine data collected through internet connectivity[23] and biometric data, such as facial recognition.[24]

The current "From the Legal Literature" column summarized two

---

[17] *Jones*, 565 U.S. at 415–16.

[18] *Jones*, 565 U.S. at 429.

[19] *Carpenter*, 138 S. Ct. at 2211.

[20] *Carpenter*, 138 S. Ct. at 2214.

[21] *E.g.*, Lauren Fash, *Automated License Plate Readers: The Difficult Balance of Solving Crime and Protecting Individual Privacy*, 78 MD. L. REV. ONLINE 63, 75–78 (2019).

[22] *E.g.*, Anne Toomey McKenna, Amy C. Gaudion, & Jenni L. Evans, *The Role of Satellites and Smart Devices: Data Surprises and Security, Privacy, and Regulatory Challenges*, 123 PENN. ST. L. REV. 591 (2019) (discussing the threat to privacy posed by aggregation of such data by smart devices).

[23] *E.g.*, Graham Johnson, *Privacy and the Internet of Things: Why Changing Expectations Demand Heightened Standards*, 11 WASH. U. JURISPRUDENCE REV. 345, (2019) (describing the privacy risks associated with the internet connectivity and arguing for a new framework that would more thoroughly protect privacy); Steven I. Friedland, *Drinking From the Fire Hose: How Massive Self-Surveillance From the Internet of Things Is Changing the Face of Privacy*, 119 W. VA. L. REV. 891 (2019) (suggesting that the "Fourth Amendment ought to be interpreted to recognize the prevalence and importance of limited purpose disclosures much like the idea of privileges used to promote certain relationships").

[24] *E.g.*, Matthew Kugler, *From Identification to Identity Theft: Public Perceptions of Biometric Privacy Harms*, 10 UC IRVINE L. REV. 107 (2019); Elizabeth Snyder, Note, *"Faceprints" and the Fourth Amendment: How the FBI Uses Facial Recognition Technology to Conduct Unlawful Searches*, 68 SYR. L. REV. 255 (2019).

articles that have applied the Court's most recent decisions to law enforcement's use of DNA data and genealogy.[25] While these two academics largely agree in their reading of Fourth Amendment doctrine, they come to varying conclusions on the particular strategies used to identify the killers discussed above. Their arguments are discussed below.

II. Antony Kolene, *"23 and Plea": Limiting Police Use of Genealogy Sites After* Carpenter v. United States, 122 W. VA. L. REV. 53 (2019).

Antony Kolene's "23 and Plea" offers two main points to the discussion of DNA data and criminal procedure. First, writing shortly after the decision in *Carpenter*, Kolene offers an exploration of the privacy interests articulated, and how those interests may affect judicial rulings on the use of DNA data.[26] Second, he suggests that the re-emergence of a property-based theory of privacy may provide greater protection against DNA searches than does the amorphous "reasonable expectation of privacy" understanding.[27]

Kolene begins his discussion with an overview of Fourth Amendment surveillance doctrine.[28] He opens with the common law prohibition on trespass and moves through the development of the *Katz* "reasonable expectation of privacy" analysis.[29] Kolene describes these two understandings, one based in property interests and the other in social expectations, as separate but concurrent tracks of Fourth Amendment analysis.[30] He notes the Court's efforts to respond to the threat posed by advancing technology in *Kyllo v. United States*[31] and the Court's apparent sensitivity to the amount of information about a person that could be mined through that technology (in the form of cell phone storage) in *United States v. Jones*[32]

---

[25] *See also* Putnam, *supra* note 5, *passim*.

[26] Kolene, *supra* note 1, at 72–100.

[27] Kolene, *supra* note 1, at 79–83.

[28] Kolene, *supra* note 1, at 57–62.

[29] Kolene, *supra* note 1, at 57–58.

[30] Kolene, *supra* note 1, at 57.

[31] Kolene, *supra* note 1, at 59; *see also Kyllo v. U.S.*, 533 U.S. 27, 34, 35, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001) (holding the use of thermal imaging devices and seminar sense-enhancing technology to gather information within a private home that could not otherwise be obtained without a physical intrusion violates the Fourth Amendment).

[32] Kolene, *supra* note 1, at 59; *U.S. v. Jones*, 565 U.S. 400, 404–11, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012) (holding that trespassing onto private property to attach a GPS tracking device to a vehicle violated the Fourth Amendment).

and *Riley v. California*.[33] He also describes, very briefly, the third party doctrine, which states that "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."[34]

Kolene then gives a very basic overview of the *Carpenter* decision. He notes that, in *Carpenter,* the Court found a situation where the expectation of privacy in physical movements (established in *Jones* and *Knotts*), comes in direct conflict with the third party doctrine.[35] Not only did the Court expressly determine that there existed an expectation of privacy against the "near perfect surveillance" of cell phone location data, it refused to limit that expectation based on the third party doctrine.[36] Noting that Justice Gorsuch specifically alluded to DNA in his dissent, Kolene suggests that this case should have repercussions for the use of genealogical research by law enforcement as well.[37]

To highlight this point, Kolene dives into an explanation of DNA, its utility for identification, and the various sources of DNA databases.[38] These databases include not only the commercial services like 23 and Me or Ancestry.com, but also government run databases made up of DNA samples taken from suspects upon arrest, or picked up at crimes scenes.[39] This is a reminder of the millions of searchable samples that currently exist, and therefore the potential extent and capabilities of genealogical surveillance.

Kolene then proceeds to analyze whether the use of this data

---

[33]Kolene, *supra* note 1, at 59–60; *see also Riley v. California*, 573 U.S. 373, 385–86, 134 S. Ct. 2473, 189 L. Ed. 2d 430, 42 Media L. Rep. (BNA) 1925 (2014) (requiring police to obtain a warrant to search the contents of a cell phone).

[34]Kolene, *supra* note 1, at 59; *see also U.S. v. Miller*, 1976-1 C.B. 535, 425 U.S. 435, 442–45, 96 S. Ct. 1619, 48 L. Ed. 2d 71, 76-1 U.S. Tax Cas. (CCH) P 9380, 37 A.F.T.R.2d 76-1261 (1976) (holding that bank customers have no protectible Fourth Amendment interest in their bank records since they are disclosed to third parties, namely bank employees); *Smith v. Maryland*, 442 U.S. 735, 742–44, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979) (holding there is no reasonable expectation of privacy in telephone numbers dialed as captured and reported by a pen register because phone users voluntarily convey numerical information to telephone companies in the ordinary course of business). For empirical critiques of these holdings, however, see Christine S. A. Scott-Hayward, Henry F. Fradella, & Ryan G. Fischer, *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19 (2016); Henry F. Fradella, Weston J. Morrow,* Ryan G. Fischer, & Connie E. Ireland, *Quantifying* Katz*: Empirically Measuring Reasonable Expectations of Privacy in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289 (2011).

[35]Kolene, *supra* note 1, at 60–61.

[36]Kolene, *supra* note 1, at 61.

[37]Kolene, *supra* note 1, at 62.

[38]Kolene, *supra* note 1, at 62–66.

[39]Kolene, *supra* note 1, at 64–66.

constitutes an invasion of privacy, under *Katz* and *Carpenter.* Kolene dismisses any privacy interest in the samples populating government run databases—these, he says, have either been expressly allowed by the Court as a means of identifying suspects, or have been "abandoned," and therefore not private (a concept subject to some controversy, but, Kolene says, largely ignored in the courts).[40]

This leaves commercial or open sources databases.[41] To analyze the privacy implications here, Kolene outlines the reasoning of the *Carpenter* Court. He argues that the Court relied on five main factors to determine whether information is private: intimacy (private details such as familial, religious, or sexual associations); comprehensiveness (the detail or extent of information); expense and difficulty (the inexpense of the investigation weighs in favor of privacy rights); retrospectivity (we do not expect the government to be able to learn information about a criminal suspect even before the suspect is under investigation); and voluntariness (whether a person as affirmatively offered information into someone else's view).[42] Each of these, Kolene suggests, weighs in favor of a privacy interest in DNA samples held in DNA databases (even voluntariness, as most genealogy sites promise privacy and control of one's data).[43] This is due to the detail included in DNA samples. Whereas government databases are presumably used only for identification of suspects, commercial databases offer comprehensive and intimate biological details about "the whole of a person's genetic makeup."[44]

However, a suspect has no standing to argue that his or her privacy interest has been violated when it is not the suspect's DNA, but a relative's DNA that is found.[45] This, Kolene argues, is similar to a suspect who tries to suppress evidence found in an illegal search of a relative's house. Kolene reminds the reader that "personal rights 'may not be vicariously asserted,' " and "a search of a third party's premises or property" cannot be challenged because the suspect has no standing.[46]

Kolene also addresses the question of DNA analysis via the property based track of surveillance doctrine, as opposed to the *Katz's* reasonable expectation of privacy analysis. Here, he finds the same results—he suggests that the Court would likely recognize a property interest in a person's own cells given the facts that some

---

[40]Kolene, *supra* note 1, at 68–70.

[41]Kolene, *supra* note 1, at 71.

[42]Kolene, *supra* note 1, at 72–74.

[43]Kolene, *supra* note 1, at 74–75.

[44]Kolene, *supra* note 1, at 71.

[45]Kolene, *supra* note 1, at 75–77.

[46]Kolene, *supra* note 1, at 76.

legislatures have already recognized such an interest, genealogy companies largely state that DNA remains the property of the person who has submitted it, and courts have recognized such ownership in the past.[47] Courts likely would not recognize a property interest in relatives' DNA, however, as "[n]o accepted principle of property law would support the notion that one person 'owns' another person's DNA as a matter of natural right."[48]

But, up until this point, Kolene has delayed addressing the third party doctrine. In part IV, Kolene reaches this discussion. He gives a brief overview of its history[49] before turning to *Carpenter*'s impact.[50] While the Court in *Carpenter* did not overturn the doctrine, it exempted cell site location data based on the extent of privacy concerns implicated and the argument that the data is not knowingly shared with others (as, the Court appears to argue, it was knowingly shared in *Smith* and *Miller*).[51] While the extent of privacy invasion is clearly extreme,[52] Kolene suggests that the level of voluntariness with which information is provided to genealogy websites negates even this privacy protection (at least under a *Katz* expectation of privacy analysis).[53] This is because all genealogy websites (even, as of recently, GEDmatch) require registration, post privacy policies online, and allow users to modify the amount of control they maintain over their data.[54] The number of express permissions users are required to give makes it difficult to argue, as was the case with cell site location data, that the relevant information was turned over unknowingly.

In contrast, Kolene argues, a property based understanding would offer greater protection even in under the third party doctrinal analysis.[55] This is because "a protected property interest [is] at stake" and "the owner of the property has merely created a bailment . . . to hold the DNA data in trust . . . A trespass on that data is still a trespass on a current property interest owned by the user."[56] This means that, while the third party doctrine would still overwhelm the *Katz*-based privacy interests articulated above, a property based

---

[47]Kolene, *supra* note 1, at 80–81.

[48]Kolene, *supra* note 1, at 83.

[49]Kolene, *supra* note 1, at 85–87.

[50]Kolene, *supra* note 1, at 87.

[51]Kolene, *supra* note 1, at 87–88.

[52]Kolene, *supra* note 1, at 97

[53]Kolene, *supra* note 1, at 98.

[54]Kolene, *supra* note 1, at 90–95, 98 (discussing privacy policies).

[55]Kolene, *supra* note 1, at 99–100.

[56]Kolene, *supra* note 1, at 100.

understanding of the Fourth Amendment might provide protection against searches of suspects' DNA (if not that of their relatives).

Even under this analysis, Kolene finds no protection against law enforcement searches of relatives' DNA. He finds this to be a problem, as these searches might enable discrimination, biological determinism, and frightening levels of simple error.[57] As he finds no real protection in Constitutional doctrine, even in light of *Carpenter*'s expansion of Fourth Amendment protections, he suggests that legislative oversight is necessary.[58]

III. GEORGE M. DERY, III, *CAN A DISTANT RELATIVE ALLOW THE GOVERNMENT ACCESS TO YOUR DNA?* 10 HASTINGS SCI. & TECH. L.J. 103 (2019).

Like Kolene, George M. Dery III, explores the application of *Carpenter* to police searches of genealogy databases. Dery begins with more detailed exploration of recent cases,[59] and less detailed exploration of established Fourth Amendment doctrine and history.[60] Like Kolene, Dery suggests that the Court's prior ruling on DNA analysis in *Maryland v. King*[61] is not controlling, as it is limited to "junk" DNA that can be used only to identify a suspect, and cannot offer the biological details that are available in full DNA samples.[62] Additionally, Dery points out the *King* Court's reliance on the idea that suspects who are in police custody have diminished expectations of privacy[63] and the historical right of police to conduct a search as part of any arrest.[64]

Unlike Kolene, Dery frames the *Carpenter* decision wholly in reference to the third party doctrine. Before moving to his discussion of *Carpenter*, he offers a more expansive discussion of the principles and reasoning underlying the third party doctrine,[65] and he introduces *Carpenter* not as a development in the legal analysis of a reasonable expectation of privacy, but as "[t]he Court's latest pronouncement on the third party doctrine."[66] But the factors Dery pulls from the opinion echo those Kolene identified. Dery focuses on the

---

[57]Kolene, *supra* note 1, at 102–03.

[58]Kolene, *supra* note 1, at 104–106.

[59]Dery, *supra* note 3, at 105–08, 111–16.

[60]Dery, *supra* note 3, at 108–11.

[61]Dery, *supra* note 3, at 116–21 (citing *Maryland v. King*, 569 U.S. 435, 449–64, 133 S. Ct. 1958, 186 L. Ed. 2d 1 (2013) (holding that a search using a buccal swab to obtain defendant's DNA sample after an arrest for a serious offense is reasonable under Fourth Amendment).

[62]Dery, *supra* note 3, at 119.

[63]Dery, *supra* note 3, at 119.

[64]Dery, *supra* note 3, at 120.

[65]Dery, *supra* note 3, at 121–24.

[66]Dery, *supra* note 3, at 123.

Carpenter Court's limiting of the third party doctrine,[67] and its emphasis on the comprehensiveness, intimacy, and retrospective nature of information provided by cell cite location data.[68] He also notes the weight the Court gave to the reach and capabilities of police technology,[69] and the "necess[ity] today that people 'compulsively carry cellphones with them all the time,' " (directing attention to whether this data can be said to be voluntarily exposed to the public).[70] After noting how perfectly the language of the Court in *Carpenter* might describe genealogical research ("If a cellphone is 'almost a feature of human anatomy,' DNA is quite literally a feature of human anatomy"),[71] Dery addresses the third-party consent hurdle to Fourth Amendment protection.

Dery offers a deeper exploration into third party consent to searches than does Kolene and comes to largely differing conclusions. Rather than understanding the principle as a purely property based doctrine, Dery brings out the doctrinal emphasis on "widely shared social expectations" and understandings of privacy, as well as the suspect's assumption of the risk of search.[72]In contrast to searches of shared rooms, suspects cannot be said to have assumed the risk of sharing their DNA with relatives who upload the data to genealogy websites. One cannot choose not to share DNA with relatives, and one cannot control what relatives do with their own DNA data.[73] And, although genealogy sites are too new to have developed "widely shared social expectations" regarding their use, Dery argues that eventually such expectations "will likely forbid one person giving the government permission to use shared DNA against a relative."[74]

Having determined that the third party consent doctrine likely would not allow for genealogical searches of relatives' DNA, Dery moves on to the question of whether such searches might be viewed as government use of a private intrusion (government use of a search conducted by a suspect's relative).[75] Dery notes the Court's prior determinations that the government may use evidence that is the result of a third party's invasion of the suspect's privacy—for instance when a private party opens a suspect's packages

[67]Dery, *supra* note 3, at 125.

[68]Dery, *supra* note 3, at 125–26.

[69]Dery, *supra* note 3, at 127.

[70]Dery, *supra* note 3, at 127.

[71]Dery, *supra* note 3, at 126–28.

[72]Dery, *supra* note 3, at 130–31.

[73]Dery, *supra* note 3, at 132–33.

[74]Dery, *supra* note 3, at 133–34.

[75]Dery, *supra* note 3, at 135.

accidentally.[76] This line of cases would seem to suggest that genealogical searches might not require a warrant, as the relative uploading the data has essentially performed the search already, and the government is simply capitalizing on that intrusion.[77] Dery acknowledges that Fourth Amendment protection may be granted, if the government search goes beyond the private party's invasion, but suggests that the type of genealogical research performed in the Golden State Killer case does not seem to rise to that level of added search.[78]

Finally, Dery approaches the standing issue.[79] Here he agrees that precedent seems to undermine any opportunity to extend Fourth Amendment protection against genealogical searches.[80] This is because, under *Byrd v. United States,* standing to assert Fourth Amendment protection extends only to people who "can exclude others" from the relevant area.[81] Under this line of cases, the right to exclude is a necessary aspect of control of property, and therefore of the right to assert standing in regards to a Fourth Amendment violation.[82] After all, an individual who never could have excluded others from an area cannot have expected the area to remain private.[83] Since a person cannot exclude relatives from searching their own DNA data, standing to assert a Fourth Amendment violation against police searches through relatives' data is impossible under this property based understanding.[84]

Given the multiple contradicting lines of precedent that might influence the question of police searches of genealogy sites, Dery's conclusion is limited. Dery maintains that the ruling in *Carpenter* strongly suggests a privacy interest in DNA, even DNA data held by genealogy sites and provided by relatives.[85] This is because of the

---

[76]Dery, *supra* note 3, at 135–36.

[77]Dery, *supra* note 3, at 138.

[78]Dery, *supra* note 3, at 139.

[79]Dery, *supra* note 3, at 140.

[80]Dery, *supra* note 3, at 1340–43.

[81]Dery, *supra* note 3, at 141–42 (citing *Byrd v. U.S.*, 138 S. Ct. 1518, 1530–31, 200 L. Ed. 2d 805 (2018) (reasoning that the mere fact that a driver in lawful possession or control of a rental car is not listed as an authorized driver on rental agreement does not defeat that person's otherwise reasonable expectation of privacy under the Fourth Amendment).

[82]Dery, *supra* note 3, at 142.

[83]Dery, *supra* note 3, at 142.

[84]Dery, *supra* note 3, at 143.

[85]Dery, *supra* note 3, at 145.

depth and breadth of information provided in these DNA samples.[86] But he acknowledges that the third party consent doctrines allow openings for warrantless searches of this information, and suggests that a future Court will likely have the opportunity to simply choose which of these lines of cases it wants to follow.[87]

It remains unclear what course the U.S. Supreme Court will take when presented with this question. What is clear, however, is that the question is coming, and its resolution will have a strong impact on police departments' newly developing methods of investigation.

---

[86]Dery, *supra* note 3, at 145.

[87]Dery, *supra* note 3, at 145; *see also* Putnam, *supra* note 5, at 258–269 (suggesting potential solutions to the privacy conundrum raised by law enforcement searches of familial DNA databases).