Criminal Law

Does the Warrantless Utilization of DNA Against a Non-Consenting Third Party Violate the Fourth Amendment?


Elizabeth S. Kase


Amy Marion


Cody Lehrer


Danielle Corbisiero

With the ever-increasing consumer popularity of determining one's genetic make-up, law enforcement has found a convenient avenue, readily available on the open market, to circumvent the strictures of the Fourth Amendment.

The publicized capture of Joseph James DeAngelo (the alleged "Golden State Killer"), aided by the utilization of a commercial DNA database, is an example of such use that has concerned many members of the legal community. The use of DNA from data banks raises questions not only for the individuals who voluntarily submit their genetic material to particular websites, but also for ethicists, law enforcement and the criminal justice system as a whole. As the Golden State Killer case revealed, sites such as 23andMe.com ("23andMe"), Ancestry.com ("Ancestry") and GEDmatch.com ("GEDmatch") may offer solutions for solving cold cases. Simultaneously, however, a time is rapidly approaching when a court will have to balance society's interest in solving heinous, cold cases with protecting an individual's right to privacy of their DNA.

The premise seems straightforward: an individual contracts with and submits a DNA sample to a DNA testing company, perhaps to locate a genetic birth parent, to confirm an ethnic heritage, or to ascertain genetic risks for disease. Similar to many consumer-based contracts, DNA companies have clearly defined legal terms and conditions that the consumer consents to when entering into the agreement with the company. Under these terms and conditions, the donor waives her privacy interest in the findings.

The legal dilemma arises when, as in the Golden State Killer case, the DNA obtained is not utilized against the donor who submitted the sample DNA but rather is used by law enforcement to ascertain the identity of a third party. In Golden State, the police collected the DNA off the website GEDmatch without using a warrant and then used it to evaluate genetic traits shared by the donor to derive possible relatives. Through this DNA, along with other evidence, law enforcement was able to narrow the search to DeAngelo. Far from settled is the issue of whether the utilization of the DNA results obtained in this way violates an accused's Fourth Amendment rights. To what extent are privacy interests afforded Fourth Amendment protection when those interests intersect with the public domain and the open marketplace?

Preliminarily, the procedure for using a privately owned genealogical database is simple and is presumed to be relatively similar among all genealogical service companies. Prior to the purchase of the DNA kit, every consumer is expected to accept the Terms and Conditions, including the clause regarding the privacy of the DNA submitted. By using such service, the DNA donor agrees to the terms associated with each website.

Ancestry and 23andMe are two of the more recognizable private genealogical database websites. They allow donors to purchase autosomal markers to predict the donor's family history and genetic ethnicity, and even provide a donor with potential DNA matches to other persons in the company's database.[1] The terms and conditions of each company state that the donor's DNA may be available to law enforcement under certain circumstances—namely, if the company believes it is necessary to comply with legal process, enforce their terms of service, or protect the company, services, employees, users, or property.[2] GEDmatch is distinguished from Ancestry and 23andMe. Unlike these two services, GEDmatch is free and more critically, open sourced. The GEDmatch consumer allows their DNA profile to be available to the public domain; DNA profiles are more easily searchable than Ancestry and 23andMe, which are private domains. Moreover, whereas the terms and conditions set out in Ancestry and 23andMe anticipate that legal process would need to be followed to obtain DNA data possessed by these two companies, GEDmatch takes pains to warn its users about law enforcement's potential use of its databank.

The publicized capture of Joseph James DeAngelo (the alleged "Golden State Killer"), aided by the utilization of a commercial DNA database, is an example of such use that has concerned many members of the legal community.

According to the GEDmatch Terms of Service and Privacy Policy, when an individual uploads the raw DNA to GEDmatch, they agree that the DNA may be designated as DNA obtained and authorized by law enforcement to identify a perpetrator of a violent crime or identify the remains of individuals.[3]

While law enforcement certainly has another potential crime fighting tool in these DNA databases, the Supreme Court's decision in *Carpenter v. United States* could place some much-needed restrictions on its usage if *Carpenter* is extended to require law enforcement to secure a warrant to use DNA data against a non-donor party.[4] In *Carpenter*, a case involving access to cell phone records, the Supreme Court held that a search is deemed conducted under the Fourth Amendment when the government accesses cell phone records that provide a comprehensive timeline of a user's movements.[5] There, law enforcement obtained two court orders directing defendant Carpenter's wireless carriers to disclose the location of Carpenter's cell phone over the four-months a set of robberies took place after receiving a confession from an accomplice naming

See DNA, Page 26


vitstudio via depositphotos.com

DNA ...

Continued From Page 8

Carpenter as a leader in the operation.[6] With these records, the government was able to confirm Carpenter's attendance at each robbery location during the specific time the robberies took place.[7]

Before trial, Carpenter unsuccessfully moved to suppress the cell-site data supplied by the wireless carriers on the grounds that the government's seizure of Carpenter's phone records violated the Fourth Amendment.[8] Carpenter argued that the records were obtained without a warrant supported by probable cause.[9] Ultimately, Carpenter was sentenced to more than 100 years in prison following several firearm convictions.[10]

On appeal, Chief Justice Roberts followed two lines of case law to resolve the issue of whether the government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.

The first line of cases concerned a "person's expectation of privacy in his physical location and movements"[11]while the second set of cases addressed the "line between what a person keeps to himself and what he shares," referred to as the Third-Party Doctrine.[12]

Addressing a person's expectation of privacy in their physical location and movements, the court looked to *United States v. Knotts* and *United States v. Jones*. In *Knotts,* the court held that , the use of a "beeper" to aid the tracking of a vehicle in traffic was not a search because people in automobiles on public roadways have "no reasonable expectation[s] of privacy in [their] movements."[13] Whereas, in *Jones*, the Court held that the FBI's use of a GPS system to track a vehicle's movements over 29 days constituted a search.[14]

So what about actual DNA? If a cell phone is a feature of human anatomy requiring a heightened expectation of privacy, DNA—a literal feature of human anatomy—would clearly imply an even more heightened expectation of privacy.

Addressing the second line of cases, the court observed that in *United States v. Miller,* no Fourth Amendment violation occurred for subpoenaed bank records because checks are negotiable instruments, not confidential communications, which the user knows are frequently used in commercial transactions and are exposed to the bank during the ordinary course of business.[15]

On similar grounds, the court held in *Smith v. Maryland*, that a device that recorded outgoing phone numbers dialed from a landline was not a search given the limited capabilities of the device, the lack of expectations regarding the privacy in the numbers people dial, and the understanding that users know telephone numbers are often used for legitimate business purposes.[16]

Addressing the facts specific to *Carpenter*, the Court found that a legitimate expectation of privacy did exist in the recording of the defendant's physical movements.[17] Finding that if society expects the government to refrain from secretly monitoring and cataloguing every movement of an individual's car, surely the comprehensive chronology contained in the records of a user's cell phone, a device referred to by the Court as "a feature of human anatomy,"–presumes a heightened expectation of privacy and Fourth Amendment protections.[18]

So what about actual DNA? If a cell phone is a feature of human anatomy requiring a heightened expectation of privacy, DNA—a literal feature of human anatomy—would clearly imply an even more heightened expectation of privacy. It is difficult to imagine that society accepts the notion that an unsuspecting consumer can simply waive a Fourth Amendment privilege belonging to a separate, unsuspecting third-party victim.

As is the case with many areas of jurisprudence, expanding technology leaves courts grappling with new and difficult fact patterns that only the test of time will resolve.

Elizabeth Kase is the Chair of the Criminal Law Department and Co-Chair of the Medical Marijuana Law Group at Abrams, Fensterman. Amy Marion is a Partner in the Litigation Division at Abrams, Fensterman. Cody Lehrer and Danielle Corbisiero are third-year law students at Hofstra University.

1. Ancestry Privacy Statement, ANCESTRY, (April 30, 2018), *https://www.ancestry.com/cs/legal/privacystatement* ("If we are compelled to disclose your Personal Information to law enforcement, we will do our best to provide you with advance notice, unless we are prohibited under the law from doing so. In the interest of transparency, Ancestry produces a Transparency Report where we list the number of valid law enforcement requests for user data across all our sites."); *See* Terms of Service, 23ANDME, (last visited September 11, 2018), https://www.23andme.com/about/tos/; *See* Privacy Highlights, 23ANDME, (July 17, 2018), https://www.23andme.com/about/privacy/.
2. *See* Ancestry Terms and Conditions, ANCESTRY, (June 5, 2018), https://www.ancestry.com/cs/legal/termsandconditions.
3. *See* GEDmatch.com Terms of Service and Privacy Policy, GEDMATCH, (May 20, 2018), https://www.gedmatch.com/tos.htm.
4. 138 S.Ct. 2206 (2018).
5. *Id.* at 2220.
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.*
10. *Id.* at 2213.
11. *Id.* at 2215.
12. *Id.* at 2216. "The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another." *Id.* at 2219.
13. 460 U.S. 276, 281 (1983).
14. *United States v. Jones,* 565 U.S. 400, 402-405 (2012).
15. *See Carpenter,* 138 U.S. at 2216.
16. 442 U.S. 735, 742-43 (1979).
17. *Carpenter, 138 U.S.* at 2217.
18. *Id.* at 2218.