The Heritage Foundation

LEGAL MEMORANDUM

No. 273 | OCTOBER 29, 2020

EDWIN MEESE III CENTER FOR LEGAL & JUDICIAL STUDIES

The Fourth Amendment Does Not Require Law Enforcement Officials to Get a Warrant to Search Third-Party Consumer Genetics Websites

Charles D. Stimson

KEY TAKEAWAYS

The consumer genetics industry has given individuals the opportunity to learn about their family heritage, genetic identity, and health risks they may have.

When consumers voluntarily contract with genetics companies, get a report, and post it to a third-party public website, they knowingly expose private information.

The Fourth Amendment does not prohibit law enforcement from accessing this information without a warrant and using it in criminal investigations.

"What's left of the Fourth Amendment?" That is the question asked by Associate Justice Neil Gorsuch in his dissent in the 2018 case of *Carpenter v. United States*.[1] The majority held that police may not collect historical cell-site location information (CSLI) from a mobile phone provider without a search warrant, at least when the police seek seven days or more of that information.[2] But the holding has broader implications well beyond CSLI. It marks a key inflection point in Fourth Amendment jurisprudence, protection of privacy, and the ever-changing role of technology in our everyday lives.[3]

The decision in *Carpenter* may require the police to get a warrant for a host of information that are in the hands of third parties.[4] However, there are limits to its reach, and certain items, voluntarily and knowingly provided to third parties, fall outside the warrant requirement of *Carpenter*. The focus of this

paper is one of those areas: third-party private websites that post forensic genetic genealogy (FGG) information available to the public including law enforcement agencies.

The consumer genetics industry has exploded in recent years, in large part because the cost of conducting genetic testing has fallen dramatically and consumers are yearning to find out more about their lineage.[5] According to a 2019 *MIT Technology Review* article, more than 29 million consumers had added their DNA to four leading commercial ancestry and health databases.[6] The two leading direct-to-consumer (DTC) genetic testing companies, Ancestry.com and 23andMe, account for the largest portion of the marketplace.[7]

A majority of consumers who voluntarily use and receive reports from DTC genetic testing companies take the additional step of posting that information to a third-party website, like GEDMatch, to get additional information about their distant relatives. GEDMatch, Parabon Nanolabs, and other third-party websites allow anyone (including law enforcement officials) to access the non-identifying information on and post DNA profiles to those websites as long as they register. In return, the customer gets a list of distant relatives and a family tree associated with the sample.

Law enforcement agencies increasingly have posted crime-scene DNA from perpetrators of crime to these public websites in the hopes that they can find a distant relative of the criminal, and this has yielded results. That is how, for example, authorities recently cracked the Golden State Killer case.[8]

Privacy advocates and legal scholars have called into question the constitutionality of this method, called long-range familial searching. They have also suggested that *Carpenter* requires law enforcement officials to get a warrant or subpoena to access such third-party public websites. For the reasons explained in this paper, those constitutional concerns lack merit, and the police should not need a warrant to access third-party, private genetics websites.

The Fourth Amendment Before *Carpenter*

The Fourth Amendment contains two clauses, one that prohibits "unreasonable searches and seizures" and another specifying the requirements for a search warrant. The text does not prohibit warrantless searches and seizures, but the Supreme Court of the United States has construed it to make such conduct presumptively unlawful.

The amendment, however, protects against searches and seizures conducted by the government, so it does not violate the Fourth Amendment

if your neighbor rummages through your garage and borrows your lawn mower without a warrant or your permission. Accordingly, there is a line distinguishing between conduct attributable to the government and conduct that is attributable to private parties, and it is only the former that raises a potential Fourth Amendment issue.

The answer to the question of whether the government has conducted a "search" often depends on whether a court believes, pursuant to a two-part test derived from a concurring opinion by Justice John Marshall Harlan II in the 1967 Supreme Court case of *Katz v. United States*, that the government has intruded on an individual's reasonable expectation of privacy.[9] In *Katz*, the majority held that the Fourth Amendment "protects people, not places,"[10] and is not dependent on intrusion into physical spaces, overturning the trespass doctrine the Court had previously established in *Olmstead v. United States*.[11] The two-part test, which has become the touchstone since *Katz*, is (1) did the affected individual have an actual (subjective) expectation of privacy, and (2) is that expectation one that society is prepared to recognize as reasonable.[12]

Two developments that largely began in the 19th century but accelerated in the 20th—specifically, the transition from what was principally an agricultural economy to a commercial one and sense-improving advances in technology—have complicated Fourth Amendment law. We now give third parties (e.g., banks and credit card companies) an enormous amount of information about ourselves in order to engage in commerce, and we have enhanced our senses' ability to see and hear at a distance utilizing emerging technologies (e.g., spotlights, microphones, and mobile phones). One result is that the government and private parties now have the ability to intrude on our privacy with information we voluntarily turn over to them or at a distance in ways that the Framers could not have contemplated.

Some of these ways create no problem.[13] Others do.[14] The question is: How do we draw the line between them?

As technology has become more advanced, giving consumers (and the government) tools that can measure, track, and record the most intimate aspects of our private lives, the Court has had to grapple with how to square rights guaranteed under the Fourth Amendment with traditional notions of privacy. The Court has taken an incremental approach, solving each case by trying to apply the Fourth Amendment to the newest technology.

In 2001, the Court found in *Kyllo v. United States*[15] that the police violated the Fourth Amendment when they used a thermal imaging device to detect heat from private areas of a suspect's home that was generated by heating lights designed to help grow marijuana indoors. Authored by Justice Antonin Scalia, the nub of the Court's majority decision was this:

> We think that obtaining by sense enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical "intrusion into a constitutionally protected area," constitutes a search—at least where (as here) the technology in question is not in general public use.[16]

In 2012, the Court delved back into the Fourth Amendment and yet another technological advance, global positioning systems (GPS), in *United States v. Jones*.[17]

GPS technology made tracking someone's vehicle far easier than it had been. Previously, the police had to follow an individual who was "on the move" in an automobile in one or more cars by conducting what is known in the vernacular as a "tail." That was constitutionally permissible. As the Court wrote in 1983 in *United States v. Knotts*, "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[18]

In *Jones*, the government obtained a search warrant to attach an electronic tracking device within 10 days to a Jeep registered to Antoine Jones's wife in the District of Columbia. The police, however, did not attach the device within those 10 days. Then, on the 11th day, after the warrant had expired, they attached a GPS tracking device to the undercarriage of the Jeep located in Maryland, and over the next 28 days, the government used the device to track the vehicle's (and Antoine Jones's) movements. The tracking device provided the government with data about the vehicle's location within 50 to 100 feet. It relayed more than 2,000 pages of data over the four-week period.

Writing for the majority, Scalia stated that "the Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted," citing the 18th century case of *Entick v. Carrington*.[19]

According to Professor Orin Kerr, a noted Fourth Amendment scholar, the Court's decision was a surprise both because the Court was unanimous as to the result and because the Justices split almost evenly along two equally underdeveloped rationales. Scalia's majority opinion, joined by four other Justices, decided the case by purporting to rediscover a lost trespass test in Fourth Amendment law. Because installing a GPS device on the car would have been a trespass under 18th century property law, Scalia asserted, the installation was a search.[20]

According to Kerr, the two concurring opinions in *Jones* suggested even more dramatic and far-reaching changes. Joined by a total of five Justices,

the two concurring opinions—one by Justice Sonia Sotomayor, who also joined Scalia's decision, and one by Justice Samuel Alito, joined by three other Justices—offer a reconceptualization of the basic building block of Fourth Amendment analysis: Instead of asking whether individual government intrusions are searches, they suggest, the Court should look to whether aggregated acts of evidence collection and evidence are searches.[21]

In her concurrence, Sotomayor noted the deeply revealing nature of the information that detailed location data can disclose, such as one's "familial, political, professional, religious, and sexual associations."[22] As discussed below, the "deeply revealing nature" of the collected information would later become the first factor in the three-part test announced in *Carpenter*, and the two concurring opinions in *Jones* later formed the basis for the majority opinion in *Carpenter*.

At least one scholar noted that the decision in *Jones* marked the beginning of the erosion of the third-party doctrine: [E]even though the Court based its ruling on a government trespass...certain Justices were clearly troubled by the constancy of surveillance enabled by the device."[23]

Then, in 2014, the Court ruled unanimously in *Riley v. California*[24] that the police generally may not without a warrant search digital information on a cell phone seized from an individual who has been arrested. The decision was a "major endorsement of treating computer searches differently than physical searches."[25] Chief Justice John Roberts, who wrote the majority opinion in *Riley*, presented the challenge for the Court: the need to decide "how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[26]

Prior to *Riley*, the search incident to arrest exception to the warrant requirement had been cemented into Supreme Court precedent since 1914[27] and was adopted, as were many other principles, from English common law. For example, the Court upheld the search of a house incident to arrest in *Chimel*,[28] a cigarette package found in the coat of the person arrested in *Robinson*,[29] and a person's vehicle (when the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search) in *Gant*.[30]

To the Chief Justice and the other Justices, however, cell phones are just different. As the Chief said in *Riley*, cell phones are "minicomputers" that contain "vast quantities of personal information." They are "not just another technological convenience," because they can also be called "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries,

albums, televisions, maps, or newspapers."[31] Searching a cell phone can reveal a person's Internet browsing history, a medical prescription, and bank statements as well as where a person has been. In short, Roberts warned, smart phones "hold for many Americans the privacies of life," and their contents are therefore protected by the Fourth Amendment.[32] Thus, reasoned the Court, "a search of the information on a cell phone bears little resemblance to the type of brief physical search considered in *Robinson*."[33]

The opinion in *Riley* was "just the tip of the iceberg," according to Kerr. "Computers have now generated a very different rule for searches incident to arrest: The police have to follow one rule for physical evidence and a different rule for digital evidence."[34]

But not all information contained on a computer about a person, even deeply revealing data, is subject to the protection of the Fourth Amendment, even under an expansive reading of *Carpenter*.

The New *Carpenter* Rule

The facts in *Carpenter* were not in dispute. In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and T-Mobile stores in Detroit. One of the men confessed that the group had robbed nine different stores in Michigan and Ohio. He identified 15 accomplices who had participated in the heists and gave the Federal Bureau of Investigation (FBI) some of their cell phone numbers. One of those numbers belonged to Timothy Carpenter. Based on that information, the government applied for court orders under the Stored Communications Act (SCA)[35] to obtain cell phone records for Carpenter and others.

A judge issued two orders directing Carpenter's wireless carriers—MetroPCS and Sprint—to disclose "cell/site sector [information] for [Carpenter's] telephone[ ] at call origination and at call termination for incoming and outgoing calls" during the four-month period when the string of robberies occurred.[36]

The government did not seek search warrants for the cell-site location information, but rather sought court orders pursuant to the SCA, which are subject to a lower standard than the "probable cause" standard that is necessary to obtain a search warrant. Furthermore, the government was not seeking the contents of the calls; it was seeking only the CSLI for the beginning and end of each call and the date and time of each transaction.

This information is often quite helpful to and commonly requested by prosecutors, who then try to match the cell site location of a person's calls on select days to see whether that phone was at or near the scene of a crime or

crimes. If the CSLI of a person's phone puts the phone at or near the scene of a crime on the day and time a crime happened, that is strong circumstantial evidence that the owner of the phone was there at that date and time.

MetroPCS produced records spanning 127 days, and Sprint produced two days of CSLI covering the period when Carpenter's phone was "roaming" in northeastern Ohio. In all, the government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.[37]

At his trial on charges of robbery and gun possession, Carpenter moved to suppress the cell-site data provided by the wireless carriers, arguing that the government's seizure of the records violated his Fourth Amendment rights because they were obtained without a warrant supported by probable cause. The District Court denied the motion, and the Court of Appeals for the Sixth Circuit affirmed.[38]

Relying on *Smith v. Maryland*, the Court of Appeals held that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers.[39] Quoting from *Smith*, the court noted that cell phone users voluntarily convey cell-site data to their carriers as "a means of establishing communication."[40] Therefore, the business records, "voluntarily" provided to and held by a third party, were not entitled to Fourth Amendment protection. The opinion by the appeals court was not surprising, as courts across the land, relying on the third-party doctrine and the holding in *Smith*, had issued similar rulings in similar cases.

In a 5–4 decision, the U.S. Supreme Court held that Carpenter's rights had been violated and that police may not collect historical cell-site location information from a cell phone provider without a warrant, at least when the police seek seven days or more of that information.[41] The majority opinion, written by Chief Justice John Roberts, relied in large part on the concurring opinions in *Jones*.

The majority reasoned that "requests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake."[42] Those two lines of cases are (1) those that address a "person's expectation of privacy in his physical location and movements,"[43] otherwise known as the reasonable expectation of privacy (REP) test, and (2) those where the "Court has drawn a line between what a person keeps to himself and what he shares with others,"[44] otherwise known as the third-party doctrine.

The third-party doctrine says that information a person voluntarily discloses to a third party is not protected by a reasonable expectation of privacy.[45] The doctrine traces its roots to two Supreme Court cases: *United States v. Miller*[46] and *Smith v. Maryland*.[47]

In *Miller*, the government was investigating an individual named Mitch Miller for tax evasion and subpoenaed his banks for canceled checks, deposit slips, and monthly statements. The Court rejected a Fourth Amendment challenge to the records collection on two grounds: (1) Miller could "assert neither ownership nor possession"[48] of the documents because they were "business records of the banks," and (2) 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."[49]

In *Smith*, the Court ruled that the government's use of a pen register—a device that recorded the outgoing phone numbers dialed on a landline telephone—was not a search. The Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial."[50] Furthermore, as the Court explained, such an expectation "is not one that society is prepared to recognize as reasonable."[51] Those numbers dialed were, like the bank records in *Miller*, business records and not subject to Fourth Amendment protection. Every time Smith made a phone call, he "voluntarily conveyed" the dialed numbers to the phone company by "expos[ing] that information to its equipment in the ordinary course of business."[52]

Even before the Court issued its decision in *Carpenter*, it was clear that the Justices were wrestling with how to square traditional notions of the Fourth Amendment, tied at first to property rights, with advances in modern technology. As the Court acknowledged in *Carpenter*, quoting its decision in *Kyllo*: "As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[53]

As one might expect, however, rather than make wholesale, sweeping pronouncements about the application of the Fourth Amendment to whole new classes of technology, the Court has taken an incremental approach based on the facts in particular cases that dealt with distinct technologies.[54] Kerr describes the Court's approach to technology and the Fourth Amendment as "the theory of equilibrium-adjustment."[55] He posits that the "Supreme Court adjusts the scope of Fourth Amendment protection in response to new facts in order to restore the status quo level of protection." Whether or not the Court is consciously engaged in equilibrium adjustment with respect to the Fourth Amendment and emerging technologies, it is clear that the "Chief Justice has declared in successive landmark decisions that the information age has produced technological changes that are different

in kind not merely in degree from the technology of the past," which another prominent scholar, Paul Ohm, calls Roberts's "tech exceptionalism."[56]

The fact of the matter is that the Court's decision in *Carpenter* "takes the Fourth Amendment in a new direction, adding new protections for non-content third-party business records."[57] After *Carpenter*, Professor Ohm wrote, "the third-party doctrine appears to be nearly dead."[58] However, rumors of the third-party doctrine's death may be greatly exaggerated[59] and would certainly come as a surprise to the five Justices in the majority who claimed otherwise. Describing their opinion as "narrow," the Justices in the majority in *Carpenter* went out of their way to say that the third-party doctrine is alive and well. Chief Justice Roberts wrote:

> We do not disturb the application of Smith and Miller or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security.[60]

Time will tell whether the third-party doctrine is alive or dead after *Carpenter*, but one thing will certainly be alive and well: Fourth Amendment legal challenges, based on an expansive reading of *Carpenter*, to things held in the hands of third parties that are not tied to CSLI. Before *Carpenter*, Fourth Amendment protections were tied to "places and things[61] and focused more on the "nature of the police intrusion required to obtain information than [they did on] the nature of the information obtained."[62] The Court in *Carpenter* set out on a "new path"[63] and added "protection to information because of what it may reveal."[64] But there are limits to even the most revealing pieces of information, depending on how it is revealed and who reveals it.

In the penultimate paragraph of the opinion, the Court summarized the characteristics of CSLI that led the Court to extend Fourth Amendment protections to it: (1) its deeply revealing nature; (2) its depth, breadth, and comprehensive reach; and (3) the inescapable and automatic nature of its collection. The fact that the information was collected by a third party made no difference to the majority. Moreover, although the majority did not announce a multi-part test *per se*, those three factors for all intents and purposes are clearly going to be integral to any test.

Factor One: The Deeply Revealing Nature of the Information. Is the information sought by the government, whether held by a third party or not, deeply revealing? If so, under the first prong of the *Carpenter*

test, the information more likely than not is protected by the Fourth Amendment. This factor is concerned with the intrinsic nature of the information itself.

The "deeply revealing" language came from Justice Sotomayor's concurring opinion in *Jones*, in which she expressed concern about information that could possibly suggest "familial, political, professional, religious, and sexual associations." Such information could be, and likely would be, deeply revealing.

Arguably, to fall under the ambit of the *Carpenter* holding, the information must be digital and not the type that could have been collected in the pre-digital age. It is rather like a constitutional grandfather clause: Pre-digital records and their modern equivalents are exempt.[65]

Factor Two: Depth, Breadth, and Comprehensive Reach. All three factors speak primarily to the quantity of information stored.[66] *Depth* refers to the detail and precision of the information sought.[67]

It is one thing for the police to tail a suspect in his car around the city for two or three days, hoping to find out more about his whereabouts and travel habits. It is an entirely different matter when the police, because of technology, have the ability to find out where a suspect (or at least his cell phone) has been for 28 days with the degree of precision that CSLI provides. CSLI gave the government the location of the defendant's phone, within 50 feet, in an uninterrupted stream of data. Even the most qualified police officer who has mastered the technique of tailing suspects without being spotted could not get that sort of detailed and precise information 24 hours a day for 28 straight days. But for the technology, the government just would not have been able to know that much private information about a person.

In contrast, *breadth* refers to time in two ways: how frequently the data are collected and for how long the data have been recorded.[68]

Using the police-tailing-the-suspect example, one would assume that the officer would record periodically where and when the suspect drove from one location to another. Even if he had a partner in the car with him who could write down every turn, when it happened, and where the suspect went, the frequency of the note scribbling is far less than the automatic, computer-driven recordation of the suspect's movements using CSLI.

A computer does not get tired. It does not eat, drink, or go to the bathroom. It does not work in shifts, does not have a boss to report to, and does not have a spouse or children to go home to or time sheets to fill out. But police officers get tired, must eat and drink, and have bosses and personal lives. There are physical limits to what a human can do and how long he can do it.

Technology is exceptional in that regard and one of the driving concerns in the cases from *Kyllo* to *Jones* to *Riley* and now to *Carpenter*. The ever-increasing power and scope of technology allows the government, through various government actors, to do things that it could not do before, and some of those things pierce the veil of privacy that we enjoyed prior to those technological advancements. They make possible that which it was previously impossible for humans to do on their own.

Finally, *comprehensive reach* refers to the number of people tracked in the database.[69]

In the context of CSLI, the cell phone provider is, for business-related purposes, collecting on a constant basis cell-site information for each individual phone, even if that phone signal is from another carrier.[70] Considering that there are approximately 396 million mobile device accounts in the United States (out of a population of around 326 million), that is a lot of digital data available to the government on a lot of people.[71] It is by definition comprehensive, especially when you consider that at least 95 percent of adults in the United States have a cell phone and carry it with them everywhere they go.[72]

The ubiquity of cell phones and how inextricably they are intertwined with the lives of virtually every adult American (and many non-adult Americans), was front and center in the majority opinion in *Carpenter*.

Factor Three: The Inescapable and Automatic Nature of Its Collection. Rather than focusing on the information's intrinsic nature, the third factor operates in a much more traditional mode, focusing on what the database owner and data subject have done—or could have done—with the information.[73]

In the context of using cell phones, it is impossible to use one without the phone sending a signal to a cell tower and then sending that signal along to the wireless provider, which in turn directs the call to the intended recipient.[74] In other words, like it or not, you cannot use a cell phone without triggering the creation of CSLI.

According to the Electronic Freedom Foundation, which filed an amicus brief in *Carpenter*, for a phone to receive and share much of that information—in other words, to be usable at all—it must connect with a cell tower. Every time the cell phone connects with the cell tower, that connection generates information, stored by the phone company, about the location of the tower to which the phone is connected—which would indicate, more or less, where the phone was—on a given date and time. These small bits of data constitute the CSLI that is aggregated and preserved by cell phone

providers.[75] Cell phones automatically try to connect to the nearest or strongest base station, and as users move farther away from one base station and closer to another, their phones automatically transfer the connection to the new base station.[76]

Kerr suggests that, with respect to *Carpenter*, "we need a theory of Fourth Amendment sensitive information that explains when an information transfer to the government has crossed the line from nonsearch to a search."[77] He suggests three steps for analyzing when a *Carpenter* search would occur, thereby requiring a warrant: (1) the records collected were available because of digital technology; (2) the records were created without the subject's meaningful voluntary choice; and (3) the records sought tend to reveal the "privacies of life."[78]

The key word in Kerr's second step, "meaningful," comes directly from *Carpenter*. The government argued that since Carpenter knowingly used his phone, he had to know that he was sharing his location information with a company in order to make the phone work. Therefore, since the location information was in the hands of a third party (his cell phone provider), the third-party doctrine applied, and the government did not need a warrant to access the CSLI.

Chief Justice Roberts was not buying it. He had been wary of the power of technology and its increasing penetration into our private lives for some time. In his view, and in that of the Justices who joined his opinion, Carpenter was not voluntarily disclosing his CSLI in a "meaningful sense."[79] Cell-site location tracking was inescapable. The records were created automatically whenever the phone was used,[80] and cell phones had become "such a pervasive and insistent part of daily life that carrying one is indispensable to participation in modern society."[81] "Apart from disconnecting the phone from the network," the Chief Justice explained, "there is no way to avoid leaving behind a trail of location data."[82]

Criminals Have No Reasonable Expectation of Privacy in Evidence They Abandon at a Crime Scene

In *California v. Greenwood*, the Supreme Court held that garbage placed at the curbside is unprotected by the Fourth Amendment.[83] The Court held that the defendant had no reasonable expectation of privacy for trash deposited on public streets that was "readily accessible to animals, children, scavengers, snoops, and other members of the public." Police cannot be expected to ignore criminal activity that can be observed by "any member of the public."

In the context of discarded DNA,[84] state courts have used the holding in *Greenwood* to permit the collection of genetic material not only from crime scenes,[85] but also from other items, such as discarded water bottles, gum, sealed envelopes, cigarette butts,[86] saliva from the mouthpiece of a passive alcohol screening device,[87] a cell phone dropped during a robbery attempt,[88] and more. Similarly, someone who leaves his blood at a murder scene may reasonably expect police to analyze it in order to ascertain the identity of the killer using all tools and technological techniques available to law enforcement agencies.

The case of *Raynor v. Maryland*[89] is an instructive illustration of how courts have treated DNA abandoned at a crime scene. In April 2006, in the early morning, an unknown male cut the victim's telephone line after chiseling open the basement door. After entering the victim's bedroom, he pressed a pillow against her face and threatened to kill her if she moved. Then, tying a shirt over the victim's face as a blindfold, he raped her and fled. During the attack, the victim noticed that her attacker had a wedding band on his hand and had a "metallicky odor."

The case was unsolved for two years. Eventually, the victim pieced together that the defendant, who used to live in the victim's home before she did, might be her attacker. She told the police, who in turn contacted Raynor, who agreed to come into the police station to be interviewed about the rape.

The police asked Raynor to consent voluntarily to providing his DNA to see whether it matched the DNA collected from the crime scene. He refused. Raynor, who wore a short-sleeved shirt during the interview, was scratching himself throughout the ordeal. After he left the police station, the police swabbed the armrests of the chair on which he had been sitting. Raynor's DNA profile was found to match the DNA profile developed from the evidence taken from the pillow case and patio at the scene of the crime.

The Maryland Court of Appeals (the state's highest court) held that the "analysis of the 13 identifying loci within Raynor's DNA left behind on the chair at the police station, in order to determine a match with the DNA the police collected from the scene of the rape, was not a search" under the Fourth Amendment. Because there is no reasonable expectation of privacy in the DNA abandoned by a criminal at a crime scene, the government's action in collecting and testing those abandoned samples was not a search within the meaning of the Fourth Amendment.

Fourth Amendment Rights Are Personal Rights

Fourth Amendment rights are personal rights that may be asserted only by a defendant who has a legitimate expectation of privacy in the invaded space or the thing searched.[90] "The established principle," according to the Supreme Court, "is that the suppression of the product of a Fourth Amendment violation can be successfully urged only by those whose rights were violated by the search itself, not by those who are aggrieved solely by the introduction of damaging evidence."[91]

Thus, to succeed on a motion to exclude evidence based on a claim of unreasonable search and seizure, a defendant must first establish a personal, reasonable, and legitimate expectation of privacy in the particular area searched or thing seized.[92] In *Kyllo*, *Jones*, *Riley*, and *Carpenter*, each defendant claimed that the government violated his Fourth Amendment rights by searching his home, car, cell phone, and CSLI, respectively.

Simply being a target of an investigation does not create a legitimate expectation of privacy for a defendant.[93] Even grossly unreasonable police conduct cannot alter the defendant's need to show that the alleged misconduct violated his personal, reasonable, and legitimate expectation of privacy.[94] Thus, for example, if a police officer were secretly to intercept a briefcase belonging to a third party and copy its contents, the defendant could not claim that his Fourth Amendment rights had been violated even if the information that was copied implicated him in a crime. In other words, there are no vicarious rights under the Fourth Amendment.[95]

Government DNA Databases

The DNA Identification Act of 1994[96] established the National DNA Index System (NDIS), which stores DNA profiles.[97] NDIS is one part of the Combined DNA Index System (CODIS)—the national part—and is the generic term used to describe the FBI's program of support for criminal justice DNA databases, as well as the software used to run these databases.[98] All 50 states, the District of Columbia, the federal government, the U.S. Army Criminal Investigative Laboratory, and Puerto Rico contribute samples to the database.[99]

The DNA Identification Act specifies the categories of data that may be maintained in the NDIS, including convicted offenders, arrestees, legal detainees, forensic casework, unidentified human remains, missing persons, and relatives of missing persons, as well as requirements for participating forensics laboratories relating to quality assurance, privacy,

and expungement.[100] Once a match is identified by the CODIS system, the laboratories involved in the match share information to verify the match and identify the individual.[101] The only information contained in the CODIS database is an identifier of the contributing agency, a unique specimen identification number, the laboratory associated with analysis, and the DNA profile.[102]

Several basic steps are performed during DNA testing regardless of the type of test being done.[103] There are several different types of forensic DNA analyses,[104] but the CODIS system uses the short tandem repeat (STR) technology to identify individuals. STR is a forensic analysis that evaluates specific regions (loci) that are found on nuclear DNA.[105] The variable (polymorphic) nature of the STR regions that are analyzed for forensic testing is used to further differentiate one DNA profile from another.[106] For example, the likelihood that any two individuals (except identical twins) will have the same 13-loci DNA profile can be as high as one in one billion or greater.[107]

The FBI initially used 13 specific STR loci to serve as the standard for CODIS. The purpose of establishing a core set of STR loci is to ensure that all forensic laboratories can establish uniform DNA databases and, more important, share valuable forensic information. If the forensic or convicted offender CODIS index is to be used in the investigative stages of unsolved cases, DNA profiles must be generated by using STR technology and the specific 13 core STR loci selected by the FBI.[108] As of January 1, 2017, however, the FBI added seven additional core loci to CODIS.[109]

The CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee.[110] Even if non-coding alleles could provide some information in that regard, they are not in fact tested with that objective in mind.[111]

Private Consumer Genetics Databases

In contrast, finding out more about your genetic roots is the whole point of the consumer genetics industry, which has exploded in recent years in large part because the cost of conducting genetic testing has fallen dramatically and consumers are yearning to find out more about their lineage.[112] According to an article in *MIT Technology Review*, by the start of 2019, more than 29 million consumers had added their DNA to four leading commercial ancestry and health databases.[113] The two leading direct-to-consumer (DTC) genetic testing companies, Ancestry.com and 23andMe, account for the majority of the marketplace.[114]

As a practical matter, a forensic DNA profile is usually generated by testing material left at a crime scene or on an object of interest to see whether scientists can find abandoned DNA and, if so, match that DNA profile to a known person.

In consumer genetics, a distant relative of a criminal purchases a genetics kit, submits a sample (such as saliva) to the company, and in time receives a profile of possible relatives and other information, depending on the company she selects. Eager to find out more about possible distant relatives or other information about her past, she voluntarily posts the non-identifying information to a third-party website, which in some cases is accessible to anyone, including law enforcement officials.

The majority of DTC ancestry genetic testing services rely on single nucleotide polymorphisms (SNPs, pronounced "snips"). SNPs are the most common type of genetic variation among people.[115] Each SNP represents a difference in a single DNA building block, called a nucleotide.[116]

SNP data can also reveal whether users share segments of their genomes with other users, predicting relatedness through a common ancestor.[117] This works by analyzing the percentage of overlapping bits of genetic code called "identical by descent" sections that one shares with relatives.[118] According to 23andMe, one likely shares roughly 12 percent of his genome with first cousins, about 3 percent with second cousins, and less than 1 percent with third cousins.[119] The probability of detecting cousins is 100 percent for first cousins; more than 99 percent for second cousins; around 90 percent for third cousins; around 45 percent for fourth cousins; about 15 percent for fifth cousins; and less than 5 percent for sixth cousins and beyond.[120]

23andMe offers consumers three services for a fee.[121] Their reports are quite detailed and give the consumer more information about her past than she had to begin with.[122] Ancestry.com offers similar services to inquisitive customers.[123]

Both 23andMe and Ancestry.com allow customers to download their raw genetic data in a plain text format.[124] Raw genetic information contains sensitive personal information, and DTC companies advise customers to protect such information. That is why most DTC companies require law enforcement to obtain a warrant to access these reports, as those reports—like government DNA databases—contain highly discriminatory information that identifies an individual via the genetic profile. What customers do with that report and how they use the information are up to them.

In addition, 23andMe's and Ancestry.com's terms of service state that they will not disclose a user's genetic data without a legal subpoena or warrant and that users cannot submit samples under an alias.[125]

Up to 62 percent of DTC customers upload their genetic data to third-party websites for free or for a small fee.[126] One of the more well-known such companies is GEDMatch. GEDMatch's purpose is to provide DNA and genealogy tools for comparison and research purposes.[127] Customers can upload raw SNP data to GEDMatch, and after the data are analyzed, the site produces a list of likely relatives automatically without the need to share any underlying genetic information with that supposed relative.

GEDMatch's terms of service require that the customer register before using its service. Users can provide a real name for registration and data upload or (unlike 23andMe and Ancestry.com) provide an alias for either login or data.[128]

Taking advantage of this ability to enter data using an alias, law enforcement officials have entered DNA from crime scenes or objects associated with a "violent crime," defined as murder, non-negligent manslaughter, aggravated rape, robbery, or aggravated assault.[129] Sometimes their efforts pay off, but not in the same way that forensic DNA matching happens where there is a "match" between the unknown DNA sample from the crime scene and a known profile. Rather, law enforcement agencies receive the same information that anyone else would receive when they use a third-party website: a list of possible relatives.

In this manner, a relative's genetic data can act as a silent witness, or "genetic informant," against the person who left the DNA at the crime scene.[130] This genetic informant wordlessly guides law enforcement officers to a handful of potential suspects simply by informing them that a suspect is very likely a third cousin, nephew, or grandson of the person in the DTC database or perhaps the perpetrator himself.[131]

Police then engage in a process of elimination by, among other things, combing through public records such as birth records, death records, driver's licenses, newspaper clippings, and the like to try to put a known name (from the handful of potential suspects) at or near the scene of the crime at the date and time of the crime. Once they narrow the list down to one or two potential suspects, police can decide how best to establish affirmatively that one of them is the person who left DNA at the crime scene. This methodology, called long-range familial searching (LRFS), has produced significant results, including helping to catch Joseph James DeAngelo Jr. (aka the Golden State Killer) and assisting in resolving scores of other previously unsolved crimes.

DeAngelo was one of the most prolific serial killers in the United States. He was responsible for murdering 13 women and raping dozens more in California in the 1970s and 1980s. Known by various names, including the "Visalia Ransacker," the "East Area Rapist," and the "Original Night

Stalker," DeAngelo eluded capture, as he was deliberate, calculating, and careful not to leave a trace.[132] Over the years, law enforcement agencies entered unknown DNA, ostensibly left by the murderer/rapist, into CODIS but came up empty-handed.

Then the consumer genetics industry sprang to life, and law enforcement officials decided to use LRFS, which cracked the decades-old case wide open. Through familial searching on GEDMatch, investigators identified relatives of DeAngelo, including family members directly related to his great-great-great-great grandfather dating back to the 1800s.[133] From there, investigators built about 25 different family trees.[134] The tree that eventually linked to DeAngelo alone contained approximately 1,000 people.[135] Over the next few months, investigators used other clues like age, sex, and place of residence to rule out suspects populating those trees, eliminating suspects one by one until only DeAngelo remained.[136]

From there, they narrowed it down to the Sacramento-area grandfather using DNA obtained from material he had discarded. When questioned by authorities in April 2018, DeAngelo said that "Jerry," an inner personality, made him do the crimes, which ended abruptly in 1986.[137] But during the same interview, while he was alone in the interrogation room, he also uttered the words "I did all that," referring to 13 murders and multiple rapes about which the police had questioned him.[138] In June of 2020, DeAngelo, 74, pleaded guilty to all of the murders, closing the case.

Why *Carpenter* Does Not Apply to Third-Party Websites

Legal scholars and privacy experts have raised alarm bells over this practice and since the decision in *Carpenter* have claimed that genetic information disclosed to third-party DTC providers is subject to the Fourth Amendment.[139] They assert, among other things, that genetic information is "precisely the sort of data in which individuals may ordinarily maintain an expectation of privacy"[140] and that allowing law enforcement officers warrantless access to third-party DTC genetic databases, which they claim is currently "unfettered,"[141] circumvents their customers' reasonable expectation of privacy.[142]

As noted previously, however, the genealogical information provided by DTC companies is far different from the DNA profile analyzed by and collected in government databases. That difference has been lost on some, including at least one state representative.

Maryland State Delegate Charles Sydnor, a Democrat who represents Baltimore County, sponsored a bill to prevent "a person from performing a search of a certain DNA or genealogical data base for the purpose of identification of an offender in connection with a crime for which the offender may

be a biological relative of the individual from whom the DNA sample was acquired; and generally relating to DNA analysis."[143] Fortunately, Delegate Sydnor's bill, which would have prevented searches of public third-party genealogical websites by anyone, including law enforcement, failed.

When Sydnor introduced his bill, he said that consumers who were uploading their profiles to third-party websites were unknowingly subjecting themselves to "genetic dragnets" in providing the samples to public websites. That concern, however, has more to do with whether the consumer was able to read and understand the terms of service of the DTC company, not the privacy rights of a distant criminal relative of the consumer who might be identified by police using LRFS. One scholar put it this way: "law enforcement's use of LRFS to solve cold cases is a bogeyman.... [M]any aspects of the methodology implicate nothing new, legally or ethically, and might even better protect privacy while exonerating the innocent."[144]

There are, to be sure, many consumer genetics companies, and the list is growing, but the two with the largest market share, 23andMe and Ancestry.com, state in plain English to potential customers that they will not disclose a user's genetic data without a legal subpoena or warrant. They also do not allow users to submit samples under an alias.

Justice Neil Gorsuch, asked in his dissent in *Carpenter*, "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."[145] His question is revealing.

First, both 23andMe and Ancestry.com require a warrant or subpoena to get a user's genetic data. The concern that the Court may have to choose between allowing the government access to those DTC websites without a warrant under a *Smith–Miller* third-party doctrine theory, or require it under a *Carpenter* approach, is therefore speculative at best. The websites require a warrant or some other form of legal process such as a subpoena.

Second, Justice Gorsuch's question evinces a fundamental misunderstanding of how consumer genetics companies actually work, who uses their services, and how and when law enforcement officials engage in LRFS. Consumers pay money to DTC companies to find out more about themselves. Consumers give DTC companies their saliva and in exchange get a report related to their ancestry (or more if they buy additional services). That information is held by the company and the consumer, and no one else. No one required the consumer to purchase the service. The record is produced at the request of the consumer, unlike CSLI, which is aggregated automatically as a result of using a cell phone.

Consumers can choose to do nothing with that information. Or they can voluntarily post the raw data to a third-party vendor, like GEDMatch, in the hope that they can learn about even more distant relatives. For those companies that allow law enforcement agencies access to their websites, law enforcement officials are not "securing your DNA without a warrant or probable cause." Rather, they are taking DNA abandoned by a criminal at a crime scene and posting it to the website in the hope that the sample might possibly be connected genetically to another customer's sample.

As to the argument that genetic information is the sort of data in which individuals maintain an expectation of privacy and that any attempt to obtain such information is therefore subject to the warrant requirement of the Fourth Amendment, it fails on a number of levels.

First, there are two categories of people involved here. The first person is the criminal who abandoned his DNA at a crime scene. Once he abandoned his DNA, whether he knew he was aware that he did so or not, he lost any Fourth Amendment protections.

The second category is the consumer, who for whatever reason decides to find out more about her genealogy. The consumer willingly provides her saliva to the DTC and in exchange receives what she contracted to receive: a report that details her genealogy. If she used 23andMe or Ancestry.com and decides to take no further action with the report, her information is protected from everyone, including law enforcement agencies, as neither company posts the information to the public. Her privacy is protected, and the government, if it somehow found out about it, would need a warrant to get that information.

If, on the other hand, she decides she wants more information about her family tree, she can contract with a third-party vendor like GEDMatch. Those vendors' terms and conditions are clear; the information generated from their analysis is open to the public (minus identifying information), and anyone, including a law enforcement officer, that is a registered user can access the information even if he or she registered using an alias. The consumer, by her own choice, has shared her genealogy with the public.

Unlike the situation in *Carpenter*, where a cell phone user has no choice but to "allow" cell towers to collect massive amounts of information about the location of the phone 24/7, the consumer has a choice about whether to contract with a DTC and whether to keep that information hidden from the public. Furthermore, law enforcement's use of LRFS falls well outside the three-part test in *Carpenter*, as well as Professor Kerr's three-step framework for a *Carpenter* search.

Read narrowly, the *Carpenter* decision is about a trail of location data related to CSLI. Any time the police obtain information from massive databases assembled by private parties that reveal an accused's location information, either directly or by inference, a criminal defendant will claim that the holding in *Carpenter* requires a warrant to get that information.[146]

Genetic information can be deeply revealing (part one of the three-part *Carpenter* test). Our DNA is the essence of who we are as humans, and while the information in a DTC website has been made possible only because of technology, it reveals much about the person who voluntarily submitted the sample to the company. The fact that the consumer's distant relative, who happens to have abandoned his DNA at a crime scene, may appear in her family tree does not give the criminal suspect any standing to assert a constitutional violation. Fourth Amendment rights are personal rights, and one cannot assert them vicariously on behalf of someone else. The genealogy report is deeply revealing to the consumer who purchased the program from the DTC, not to a defendant.

Similarly, the information arguably has depth, breadth, and a comprehensive reach (part two of the three-part *Carpenter* test). But the right of privacy belongs to the consumer, not to a defendant who abandoned his DNA at a crime scene.

Finally, there is nothing inescapable or automatic about the nature of the collection of the information involved (part three of the three-part *Carpenter* test). Here, a consumer has entered into a contract requesting that a company generate a genetics report and then has taken the additional step of posting the results to a third-party website. Both acts are completely voluntary. The person using the DTC website chose to submit a DNA sample for analysis; it was not automatically collected while the individual was engaging in some other indispensable or inextricably intertwined activity such as using a cell phone in today's modern age.

Conclusion

Whether analyzed under a *Katz* reasonable expectation of privacy prism, or by applying the third-party doctrine or even stretching the boundaries of the *Carpenter* decision, law enforcement officials should not be required to obtain a warrant to search third-party genetics websites that allow for public access.

The consumer genetics industry, enabled by technology, has given consumers the opportunity to explore their lineage. When consumers voluntarily contract with DTC consumer genetics companies, receive a

genetics report, and voluntarily post that report to a third-party website that gives the public and law enforcement agencies access to the non-identifying information, they expose private information to the public. That information, including the consumer's family tree, does not give vicarious Fourth Amendment rights to distant relatives.

Law enforcement officers should not be required to get a warrant to query a public database on the off chance that they may find a distant relative of a person who abandoned his or her DNA at a crime scene.

Charles D. Stimson is a Senior Legal Fellow and Manager of the National Security Law Program in the Edwin Meese III Center for Legal and Judicial Studies, of the Institute for Constitutional Government, at The Heritage Foundation.

Endnotes

1. Carpenter v. United States, 138 S. Ct. 2206 (2018).
2. *Id.* at 2212 n.3 ("It is sufficient for our purposes today to hold that accessing seven days of [cell-site location information] constitutes a Fourth Amendment search.").
3. *See*, *e.g.*, Paul Ohm, *The Many Revolutions of* Carpenter, 32 Harv. J.L & Tech. 357 (2019); *see also* Antony Barone Kolenc, *"23 And Plea": Limiting Police Use of Genealogy Sites After* Carpenter v. United States, 122 W. Va. L. Rev. 53 (2019); Teneille R. Brown, *Why We Fear Genetic Informants: Using Genetic Genealogy to Catch Serial Killers*, 21 Colum. Sci. & Tech. L. Rev. 1 (2019); *see also* Orin Kerr, *First Thoughts on* Carpenter v. United States, Volokh Conspiracy (June 22, 2018, 12:20 PM), https://reason.com/2018/06/22/first-thoughts-on-carpenter-v-united-sta/.
4. *See* Ohm, *supra* note 3, at 378–85 (Ohm discusses three categories of third-party-collected records that are "likely to be found protected by a reasonable expectation of privacy and fall outside the third party doctrine." The three categories include: (1) very likely to be covered; (2) most likely to be covered; and (3) uncertain application, in which Ohm asks, "What about a copy of an individual's DNA stored with a private third party?" Ohm notes that Gorsuch, in his dissent, "opines without analysis that 'most lawyers and judges today' would require a warrant and probable cause to access DNA voluntarily stored with 23andMe." See *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).
5. *See* Brown, *supra* note 3, at 7.
6. *See* Antonio Regalado, *More Than 26 Million People Have Taken an At-Home Ancestry Test*, MIT Tech. Rev. (Feb. 11, 2019), https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/.
7. *Id.*
8. *See* JV Chamary, *How Genetic Genealogy Helped Catch the Golden State Killer*, Forbes (Jun. 30, 2020), https://www.forbes.com/sites/jvchamary/2020/06/30/genetic-genealogy-golden-state-killer/#3a8802b55a6d; *see also* Andrea Marks, *DNA Search Method That Caught Golden State Killer No Longer Available*, Rolling Stone (May 23, 2019), https://www.rollingstone.com/culture/culture-news/dna-search-method-that-caught-the-golden-state-killer-no-longer-available-839315/.
9. 389 U.S. 347 (1967).
10. *Id.* at 351.
11. 277 U.S. 438 (1928).
12. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (articulating the reasonable expectation of privacy test).
13. *See* United States v. Lee, 274 U.S. 559 (1927), where the U.S. Coast Guard's use of a searchlight before boarding another boat to illuminate the deck was held not to be a search. *See also* United States v. Miller, 425 U.S. 435 (1976), where the Court held that the respondent had no expectation of privacy under the Fourth Amendment with respect to bank records as they were business records of the bank, not his private papers.
14. *See* Katz, *supra* note 9, where the police, without a warrant, attached a microphone to a telephone booth to learn whether Katz, as suspected, was transmitting gambling information over the phone to clients in other states. The Court held that the police needed a warrant because the Fourth Amendment protected people, not places.
15. Kyllo v. United States, 533 U.S. 27 (2001).
16. *Id.* at 35, quoting from Silverman v. United States, 365 U.S. 505, 512 (1961).
17. *See* United States v Jones, 565 U.S. 400 (2012).
18. *See* United States v. Knotts, 460 U.S. 276, 281 (1983).
19. *See Jones*, 565 U.S. at 404–05; *see also* Entick v. Carrington 95 Eng. Rep. 807 (C. P. 1765). In his majority opinion for the U.S. Court of Appeals for the District of Columbia Circuit, Judge Douglas Ginsburg held that the police violated Jones's reasonable expectation of privacy and that the police needed a warrant to surveil him for those 28 days. Judge Ginsburg found that the Court's holding in United States v. Knotts, 460 U.S. 276 (1983), in which the Supreme Court held that the use of a beeper device to aid in tracking a suspect to his drug laboratory was not a search, did not govern as the Court specifically reserved the question whether a warrant would be required in a case involving 24-hour surveillance. The GPS device provided surveillance 24 hours a day, seven days a week, and thus required the police to get a warrant according to Ginsburg. Ginsburg's opinion in *Jones* and his approach are similar to the approach by Chief Justice John Roberts in the *Carpenter* decision as discussed herein.
20. *See* Orin Kerr, *Reviewing the Fourth Amendment Cases of OT2011*, SCOTUSblog (Aug. 7, 2012, 2:05 PM), https://www.scotusblog.com/2012/08/reviewing-the-fourth-amendment-cases-of-ot2011/.

21. *Id.*; *see also Jones*, 565 U.S. at 417–18 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.... This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as JUSTICE ALITO notes, some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,' and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.") (citations omitted).
22. *See Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).
23. *See* Joseph Zabel, *The Killer Inside Us: Law, Ethics, and the Forensic Use of Family Genetics*, 24 Berkeley J. Crim. L. 47, 54 (2019).
24. 573 U.S. 373 (2014).
25. *See* Orin Kerr, *The Significance of Riley*, Volokh Conspiracy (June 25, 2014, 11:56 AM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/25/the-significance-of-riley/.
26. *See Riley*, 573 U.S. at 385.
27. *See* Weeks v. United States, 232 U.S. 383, 392 (1914) (dictum) (citations omitted) (Court stating, "It is not an assertion of the right on the part of the government always recognized under English and American law, to search the person of the accused when legally arrested, to discover and seize the fruits or evidences of crime. This right has been uniformly maintained in many cases.") (citations omitted).
28. Chimel v. California, 395 U.S. 752 (1969).
29. United States v. Robinson, 414 U.S. 218 (1973).
30. Arizona v. Gant, 556 U.S. 332 (2009).
31. *See Riley*, 573 U.S. at 393.
32. *See Carpenter*, 138 S. Ct. at 2217 (citations omitted).
33. *See Riley*, 573 U.S. at 386.
34. *See* Orin Kerr, Implementing Carpenter, The Digital Fourth Amendment (Oxford University Press, forthcoming), *abstract available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257.
35. Section 2703(d) of the Stored Communications Act (18 U.S.C. §§2701–2712), as amended, permits the government to compel the disclosure of certain telecommunications records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." Congress passed the SCA against a background assumption that electronic data held by third parties were not covered by the Fourth Amendment because of the third-party doctrine, which provides that government acquisition of a person's data (especially non-content data) from a third party is generally outside the scope of the Fourth Amendment. *See* Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After Carpenter*, 128 Yale L.J. Forum 943 (2019).
36. *Carpenter*, 138 S. Ct. at 2212.
37. *Id.*
38. United States v. Carpenter, 819 F.3d 880 (2016) (subsequent history omitted).
39. *Id.* at 894.
40. *Id.*; *see also* Smith v. Maryland, 442 U. S. 735, 741 (1979).
41. *Carpenter*, 138 S. Ct. at 2217 n.3.
42. *Id.* at 2214–15. Others have argued that the trajectory of the Fourth Amendment had been on two different and somewhat inconsistent tracks: (1) it was traditionally tied to the common law of trespass and focused on whether the government obtained information by physically intruding on a constitutionally protected area, and (2) as a result of Katz v. United States, the Fourth Amendment protects people and their reasonable expectations of privacy, not just places. *See*, *e.g.*, Kolenc, *supra* note 3, at 57–58.
43. *Carpenter*, 138 S. Ct. at 2214–15.
44. *Id.* at 2216.
45. *See* Ohm, *supra* note 3, at 362 (quoting Orin Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 566–70 (2009)).
46. 425 U. S. 435 (1976).
47. 442 U.S. 735 (1979).
48. *Miller*, 425 U.S. at 440.

49. *Id.* at 442.
50. *Smith*, 442 U.S. at 742.
51. *Id.*
52. *Id.* at 744.
53. *See Carpenter*, 138 S. Ct. at 2271.
54. Even in Carpenter, which has broad and sweeping implications as discussed in this paper, the Court acknowledged that its members were wrestling with the dizzying pace of technological change and the application of the Fourth Amendment to that change. "We do not begin to claim all the answers today," the Chief Justice acknowledged in light of "the manifold situations that may be presented by this new technology." Claiming that their decision was narrow, the Justices asserted that they were deciding "no more than the case before us." While that may have been the Court's intent, the Carpenter decision itself is a watershed moment in Fourth Amendment jurisprudence as discussed herein. *See Carpenter*, 138 S. Ct. at 2220 n.4.
55. *See* Orin Kerr, *An Equilibrium Adjustment Theory of the Fourth Amendment*, 125 Harv. L. Rev. 476 (2011).
56. See Ohm, *supra* note 3, at 401.
57. *See* Kerr, *supra* note 32.
58. See Ohm, *supra* note 3, at 363.
59. This quote is attributed to Mark Twain. In 1897, an English journalist from the *New York Journal* contacted Twain to inquire whether the rumors that he was gravely ill or already dead were indeed true. Twain wrote a response that ran in the *Journal* on June 2, 1897: "I can understand perfectly how the report of my illness got about, I have even heard on good authority that I was dead. James Ross Clemens, a cousin of mine, was seriously ill two or three weeks ago in London, but is well now. The report of my illness grew out of his illness. The report of my death was an exaggeration." *See* Emily Petsko, *Reports of Mark Twain's Quote About His Own Death Are Greatly Exaggerated*, Mental Floss (Nov. 2, 2018), https://www.mentalfloss.com/article/562400/reports-mark-twains-quote-about-mark-twains-death-are-greatly-exaggerated.
60. *See Carpenter*, 138 S. Ct. at 2220.
61. *Id.*
62. See Ohm, *supra* note 3, at 362.
63. See Kerr, *supra* note 32 (Chapter 6, The Carpenter Shift). One could argue that this actually began with *Riley*. It used to be that police could search a phone that an arrestee had in his possession as a search incident to arrest, but because of the amount of personal information held on smartphones today, the Court held that a warrant was required.
64. *Id.*
65. *See* Kerr, *supra* note 32. This limit originates in *Carpenter* itself. According to the Chief Justice, "seismic shifts in digital technology" have "made possible" access to "an entirely different species" of data that "do[] not fit neatly under existing precedents." This created "new concerns wrought by digital technology" that were inconsistent with viewing the cell-site records as simply a new form of an old record that should be treated like the old records. Only the new records exceed society's expectation from "[p]rior to the digital age" about what "law enforcement agents and others" would or could do. "There is a world of difference," the Court concluded, "between the limited types of personal information" at issue before the digital age and the "exhaustive chronicle" of information the new technologies can provide.
66. See Ohm, *supra* note 3, at 372.
67. *Id.*
68. *Id.*
69. *Id.*
70. *See* Brief for Electronic Frontier Foundation, et al. as Amici Curiae Supporting Petitioner, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402), at 10–13, *available at* https://www.eff.org/document/amicus-brief-carpenter.
71. *Id.*
72. *Id.*
73. See Ohm, *supra* note 3, at 376.
74. See generally Brief for Electronic Frontier Foundation, et al., *supra* note 70.
75. *Id.* at 2. Cell phones send and receive radio signals via base stations, known as cell towers. Towers typically have multiple cell "sites" facing in three or four different directions, each containing antennae that detect radio signals emanating from phones and that connect the phones to the cellular network.
76. *Id.*
77. *See* Kerr, *supra* note 32.
78. *Id.*

79. *Carpenter*, 138 S. Ct. at 2220.
80. *See* Kerr, *supra* note 32.
81. *Carpenter*, 138 S. Ct. at 2220.
82. *Id.*
83. 486 U.S. 35 (1988).
84. DNA, or deoxyribonucleic acid, is the hereditary material in humans and almost all other organisms. Nearly every cell in a person's body has the same DNA. Most DNA is located in the cell nucleus (where it is called nuclear DNA), but a small amount of DNA can also be found in the mitochondria (where it is called mitochondrial DNA or mtDNA). Mitochondria are structures within cells that convert the energy from food into a form that cells can use. The information in DNA is stored as a code made up of four chemical bases: adenine (A); guanine (G); cytosine (C); and thymine (T). Human DNA consists of about 3 billion bases, and more than 99 percent of those bases are the same in all people. The order, or sequence, of these bases determines the information available for building and maintaining an organism, much as letters of the alphabet appear in a certain order to form words and sentences. DNA bases pair with each other, A with T and C with G, to form units called base pairs. Each base is also attached to a sugar molecule and a phosphate molecule. Together, a base, sugar, and phosphate are called a nucleotide. Nucleotides are arranged in two long strands that form a spiral called a double helix. The structure of the double helix is somewhat like a ladder, with the base pairs forming the ladder's rungs and the sugar and phosphate molecules forming its vertical sidepieces. An important property of DNA is that it can replicate, or make copies of itself. Each strand of DNA in the double helix can serve as a pattern for duplicating the sequence of bases. This is critical when cells divide because each new cell needs to have an exact copy of the DNA present in the old cell. *See* Genetics Home Reference, U.S. National Library of Medicine, National Institutes of Health, https://ghr.nlm.nih.gov/primer/basics/dna (last visited Aug. 5, 2020).
85. The fact that police can recover blood or other genetic material from a crime should not be surprising to most people or cause anyone concerned with solving crimes any constitutional concerns, but at least two authors have called into question the constitutionality of testing genetic material found (abandoned) at a crime scene. Elizabeth E. Joh, for example, calls the practice a "backdoor method of DNA collection" and wrote a law review article dedicated to the government's collection of abandoned DNA, which she calls a "problem worthy of serious attention." *See* Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 Nw. U. L. Rev. 857, 858 (2006).
86. California v. Gallego, 190 Cal.App.4th 388, 395–398 (2010).
87. People v. Thomas, 200 Cal.App.4th 338, 342 (2011).
88. People v. Daggs, 133 Cal.App.4th 361, 365–366 (2005).
89. 99 A.3d 753 (Md. 2014).
90. Rakas v. Illinois, 439 U.S. 128, 133–34 (1978).
91. Alderman v. United States, 394 U.S. 165, 171–72 (1969).
92. United States v. Payner, 447 U.S. 727, 731 (1980).
93. *See Rakas*, 439 U.S. at 135.
94. *See Payner*, 447 U.S. at 731–34.
95. See Brown, *supra* note 3, at 29.
96. 42 U.S.C. §14132.
97. *See Frequently Asked Questions About CODIS and NDIS, "What Is CODIS?"*, FBI.gov, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Aug. 2, 2020); *see also* Erin E. Murphy, Inside the Cell: The Dark Side of Forensic DNA 14–16 (2015).
98. *Id.*
99. *Id.*
100. *Id.*
101. *Id.*; *see also* Brown, *supra* note 3, at 17.
102. Brown, *supra* note 3, at 17.
103. The information contained in this paragraph was taken directly from the U.S. Justice Department, National Institute of Justice (NIJ) webpage, "DNA Evidence: Basics of Analyzing," https://nij.ojp.gov/topics/articles/dna-evidence-basics-analyzing (last visited Aug. 1, 2020). The general procedure includes (1) isolation of the DNA from an evidence sample containing DNA of unknown origin and, generally at a later time, isolation of DNA from a sample (e.g., blood) from a known individual; (2) processing of the DNA so that test results may be obtained; (3) determination of the variations in the DNA test results (or types) from specific regions of the DNA; and (4) comparison and interpretation of the test results from the unknown and known samples to determine whether the known individual is not the source of the DNA or is included as a possible source of the DNA. Each additional test at a previously untested locus (location or site) in the DNA provides another opportunity for the result of "exclusion" if the known individual being used for comparison is not the source of the DNA from an evidence sample of unknown origin. If, however, the known individual is the source of the DNA on the evidence sample, additional testing will continue only to include that individual as a possible source of the DNA. When a sufficient number of tests have been performed in which an individual cannot be excluded as the source of the DNA by any of the tests, a point is reached at which the tests have excluded virtually the world's population and the unique identification of that individual as the source of the DNA has been achieved.

104. *See Frequently Asked Questions*, *supra* note 97. They include (1) short tandem repeat (STR); (2) polymerase chain reaction (PCR); (3) Y chromosome analysis; (4) mitochondrial (mtDNA) analysis; and (5) restriction fragment length polymorphism (RFLP). DNA data generated through PCR Short Tandem Repeat (STR) technology, Y chromosome STR (Y STR) technology, and Mitochondrial DNA (mtDNA) technology are accepted at NDIS. Y STR and mtDNA data are searched only with the missing person–related indexes. The National DNA Index no longer searches DNA data developed using restriction fragment length polymorphism (RFLP) technology.
105. *See NIJ*, *supra* note 103.
106. *Id.*
107. *Id.*
108. *Id.*
109. *See Frequently Asked Questions*, *supra* note 97. The 20 core loci include CSF1PO, FGA, THO1, TPOX, VWA, D3S1358, D5S818, D7S820, D8S1179, D13S317, D16S539, D18S51, D21S11, D1S1656, D2S441, D2S1338, D10S1248, D12S391, D19S433, and D22S1045.
110. See Maryland v. King, 569 U.S. 435, 464 (2013).
111. *Id.*
112. *See* Brown, *supra* note 2, at 7.
113. *See* Regalado, *supra* note 6.
114. *Id.*
115. *See "What Are Single Nucleotide Polymorphisms?"*, Genetics Home Reference, U.S. National Library of Medicine, National Institutes of Health, https://ghr.nlm.nih.gov/primer/genomicresearch/snp (last visited Aug. 2, 2020).
116. *Id.* These variations may be unique or occur in many individuals; scientists have found more than 100 million SNPs in populations around the world. Most commonly, these variations are found in the DNA between genes. They can act as biological markers, helping scientists to locate genes that are associated with disease. When SNPs occur within a gene or in a regulatory region near a gene, they may play a more direct role in disease by affecting the gene's function. Most SNPs have no effect on health or development. Some of these genetic differences, however, have proven to be very important in the study of human health. Researchers have found SNPs that may help to predict an individual's response to certain drugs, susceptibility to environmental factors such as toxins, and risk of developing particular diseases. SNPs can also be used to track the inheritance of disease genes within families. Future studies will work to identify SNPs associated with complex diseases such as heart disease, diabetes, and cancer. SNPs occur normally throughout a person's DNA. They occur almost once in every 1,000 nucleotides on average, which means there are roughly 4 million to 5 million SNPs in a person's genome.
117. *See* Brown, *supra* note 3, at 11.
118. *Id.*
119. *See* DNA Relatives: Detecting Relatives and Predicting Relationships, 23andMe.com, https://customercare.23andme.com/hc/en-us/articles/212170958-DNA-Relatives-Detecting-Relatives-and-Predicting-Relationships (last visited July 25, 2020).
120. *Id.*
121. *See* Our Services, 23andMe.com, https://www.23andme.com/compare-dna-tests/ (last visited Aug. 7, 2020).
122. For an example of a 23andMe report, *see* https://education.23andme.com/example-reports/.
123. *See* ancestry.com/dna.
124. *See* Yaniv Erlich, *Identity Inference of Genomic Data Using Long Range Familial Searches*, 362 Science 690, 691 (2018).
125. *See* Terms and Conditions, ancestry.com, https://www.ancestry.com/cs/legal/termsandconditions (last visited Aug. 7, 2020); *see also* Terms of Service, 23andMe.com, https://www.23andme.com/about/tos/ (last visited Aug. 7, 2020).
126. *See* Brown, *supra* note 3, at 12–13.
127. *See* Terms of Service and Privacy Policy, GEDMatch.com, https://www.gedmatch.com/tos.htm (last visited Aug. 2, 2020).
128. *Id.*
129. *Id.*
130. *See* Brown, *supra* note 3, at 4.
131. *Id.*
132. *See* Avi Selk, *The Most Disturbing Parts of the 171-Page Warrant for the Golden State Killer Suspect*, Wash. Post, June 2, 2018, *available at* https://www.washingtonpost.com/news/post-nation/wp/2018/06/02/the-most-disturbing-parts-of-the-171-page-warrants-for-the-golden-state-killer-suspect/.
133. *See* Zabel, *supra* note 23, at 50–51.
134. *Id.*

135. *Id.*
136. *Id.*
137. *See Golden State Killer Pleads Guilty to Murders, Allegedly Said, "I Did All That"*, CBSNEWS.COM (Updated June 29, 2020, 3:36 PM), https://www.cbsnews.com/news/golden-state-killer-joseph-deangelo-pleads-guilty-murders/.
138. *Id.*
139. *See generally* Amelia Putnam, *A Genetic Panopticon of Our Own Making: How the Fourth Amendment Applies to Commercial Genealogy DNA Testing*, 56 No. 2 Crim. Law Bull., Art 2, (2020); George M. Dery III, *Can a Distant Relative Allow Government Access to Your DNA? The Fourth Amendment Implications of Law Enforcement's Genealogical Search for the Golden State Killer and Other Genetic Genealogy Investigations*, 10 Hastings Sci. & Tech. L.J., 103 (2019); Claire Abrahamson, Note, *Guilt by Genetic Association: The Fourth Amendment and the Search of Private Genetic Databases by Law Enforcement*, 87 Fordham L. Rev. 2539 (2019); Natalie Ram, *Genetic Privacy after Carpenter*, 105 Va. L. Rev. 1357 (2019).
140. *See* Ram, *supra* note 139, at 1358.
141. *See* Zabel, *supra* note 23, at 54.
142. *See* Abrahamson, *supra* note 139, at 2539.
143. H.B. 30, 440th Gen. Assembly, Reg. Sess. (Md. 2019).
144. Brown, *supra* note 3, at 6.
145. *See Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J. dissenting).
146. *See* Ohm, *supra* note 3, at 366.