GENETIC PRIVACY AFTER *CARPENTER*

Natalie Ram∗

The recent arrest of the alleged Golden State Killer has ignited law enforcement interest in using consumer genetic databases to crack cold cases. The break in that case came when investigators compared crime scene DNA to other DNA profiles searchable in an online genetic genealogy database called GEDmatch. Yet consumer genetic services have responded to law enforcement interest in markedly different ways. Some have explicitly denounced law enforcement use and vowed to oppose it; others have welcomed law enforcement expressly; and some have cooperated quietly with law enforcement, while keeping their users in the dark. At almost the same time, the Supreme Court gave these platforms a new role in policing police access to their genetic

∗ Associate Professor, University of Maryland Carey School of Law; J.D., Yale Law School; A.B., Princeton University. This work is supported by a Greenwall Faculty Scholars grant. Many thanks to Andrew Blair-Stanek, Max Blankfeld, I. Glenn Cohen, David Gray, Cynthia Ho, David Jaros, Dmitry Karshtedt, Sherri Lee Keene, Lee Kovarsky, William J. Moon, Mike Pappas, Jordan Paradise, Neil Richards, Jessica Roberts, Kevin Tu, Liza Vertinsky, and Leslie Wolf for their helpful comments on this project. This work benefitted from feedback at the Wiet Life Science Scholars Conference at Loyola Chicago School of Law, the Health Law Workshop at Harvard Law School, the University of Maryland-University of Baltimore Joint Junior Faculty Workshop, and faculty workshops at American University Washington College of Law, University of Houston Law Center, and the University of Maryland Carey School of Law. Thanks also to Mark Russell and other editors at the *Virginia Law Review* for their assistance in bringing this Article to publication. All errors are my own.

As this Article was going to press, the Department of Justice released an interim policy on "forensic genetic genealogical DNA analysis and searching." See U.S. Dep't of Justice, Interim Policy: Forensic Genetic Genealogical DNA Analysis and Searching (2019), https://www.justice.gov/olp/page/file/1204386/download [https://perma.cc/XY3C-7558]; Press Release, Dep't of Justice, Department of Justice Announces Interim Policy on Emerging Method to Generate Leads for Unsolved Violent Crimes (Sept. 24, 2019), https://www.justice.gov/opa/pr/department-justice-announces-interim-policy-emerging-method-generate-leads-unsolved-violent [https://perma.cc/2PXJ-NKJY]. This policy is not a part of the analysis below, nor does it alter this Article's reasoning or conclusions. Nonetheless, this policy acknowledges that "the requirements and protections of the Constitution and other legal authorities" may constrain law enforcement use of forensic genetic genealogy. Interim Policy, supra. Moreover, consistent with this Article, the policy instructs that law enforcement may utilize forensic genetic genealogy techniques only in those consumer genetics platforms that "provide explicit notice to their service users and the public that law enforcement may use their service sites to investigate crimes or to identify unidentified human remains." Id. (footnote omitted).

resources. In Carpenter v. United States*, the Court upended the seemingly categorical rule that one cannot have an expectation of privacy in data shared with another.*

This Article examines the impact of Carpenter *for law enforcement use of third-party DNA databases, as in the Golden State Killer case. In so doing, this Article makes three contributions. First, it joins a burgeoning scholarship in identifying* Carpenter*'s "test," and demonstrates that genetic information is precisely the sort of data in which individuals may ordinarily maintain an expectation of privacy, even when that data is in third-party hands. Second, it considers the role of consumer genetic platforms in mediating police access to their resources, recasting third-party privacy practices in a more robust and nuanced role as measures of consent. Third, it assesses the privacy practices of genetic genealogy companies specifically, concluding that some plainly reinforce existing expectations of privacy in genetic data, while others have meandered their way closer to legally valid consent to government use—though none has done so with precision.*

INTRODUCTION

On April 24, 2018, police arrested Joseph James DeAngelo, alleging that he is the elusive Golden State Killer, suspected of more than a dozen murders and nearly fifty rapes dating back more than forty years.[1] The break in the case came when investigators compared DNA recovered from victims and crime scenes to other DNA profiles searchable in a free genealogical database called GEDmatch.[2] That search turned up a distant cousin of the Golden State Killer's, and through sleuthing in that family tree, investigators eventually homed in on DeAngelo—a technique now known as "genetic genealogy."[3] Police arrested DeAngelo to great fanfare after confirming a DNA match between the crime scene evidence and DeAngelo's DNA that had been surreptitiously collected from the door handle of his car and a discarded tissue.[4]

[1] See Benjamin Oreskes, Joseph Serna & Richard Winton, False Starts in Search for Golden State Killer Reveal the Pitfalls of DNA Testing, L.A. Times (May 4, 2018), http://www.latimes.com/local/lanow/la-me-ln-golden-state-killer-dna-20180504-story.html [https://perma.cc/6JBV-HQS6]; Ray Sanchez et al., After Searching for More Than 40 Years, Authorities Say an Ex-Cop is the Golden State Killer, CNN (Apr. 27, 2018), https://www.cnn.com/2018/04/25/us/golden-state-killer-development/index.html [https://perma.cc/H9G5-FAEL].

[2] See Laurel Wamsley, In Hunt for Golden State Killer, Investigators Uploaded His DNA To Genealogy Site, NPR (Apr. 27, 2018), https://www.npr.org/sections/thetwo-way/2018/04/27/606624218/in-hunt-for-golden-state-killer-investigators-uploaded-his-dna-to-genealogy-site [https://perma.cc/77H3-XVVX]. Use of the terms "search" or "searchable" in this Article does not require that law enforcement (or other users) gain access to matching individuals' full sequence data. Rather, these terms refer to the comparison of genetic profiles to generate matches, including by means of an algorithm.

[3] See Justin Jouvenal, To Find Alleged Golden State Killer, Investigators First Found His Great-Great-Great-Grandparents, Wash. Post (Apr. 30, 2018), https://www.washingtonpost.com/local/public-safety/to-find-alleged-golden-state-killer-investigators-first-found-his-great-great-great-grandparents/2018/04/30/3c865fe7-dfcc-4a0e-b6b2-0bec548d501f_story.html [https://perma.cc/YE65-UBV3]; see also Laura Hautala, How Sharing Your DNA Solves Horrible Crimes . . . and Stirs a Privacy Debate, CNet (July 2, 2019), https://www.cnet.com/news/how-sharing-your-dna-solves-horrible-crimes-and-stirs-a-privacy-debate/# (defining this technique as "genetic genealogy"). In other work, I have described this technique as forensic, rather than merely genetic genealogy, as it puts genealogical data, including DNA, to forensic ends. See Natalie Ram & Jessica L. Roberts, Forensic Genealogy and the Power of Defaults, 37 Nature Biotechnology 707, 708 (2019). For present purposes, this Article utilizes the more popular "genetic genealogy."

[4] See Christal Hayes, Golden State Killer: Police Took DNA from Car as Suspect Shopped in Hobby Lobby, Plucked His Tissue from Trash, USA Today (June 2, 2018), https://www.usatoday.com/story/news/nation/2018/06/02/golden-state-killer-dna-car-hobby-lobby/666608002/ [https://perma.cc/7JZG-QFS2].

The case of the Golden State Killer was not the first instance of investigators turning to non-forensic DNA databases to generate leads.[5] It was not even the first time investigators used genealogical DNA matches to develop and pursue a suspect in the Golden State Killer case itself.[6] A year before investigators zeroed in on DeAngelo, they subpoenaed another genetic testing company for the name and payment information of one of its users and obtained a warrant for a different man's DNA.[7] He was not a match.[8] Similarly, in 2014, Michael Usry found himself the target of a police investigation stemming from a partial genetic match between his father's DNA, stored in a then-publicly searchable Ancestry database, and DNA left at a 1996 murder scene.[9] Based on the partial match, police were able to obtain a court order requiring Ancestry to disclose the identity of the database DNA match.[10] After mapping out several generations of Usry's father's family, investigators zeroed in on Usry, eventually securing a warrant for his DNA.[11] Ultimately, Usry was cleared as a suspect when his DNA proved not to match the crime scene DNA.[12] But there were also other reported successes. In 2015, for example, Arizona police arrested and charged Bryan Patrick Miller in the Canal Killer murders based in part on a tip drawn from a genealogical database search.[13]

Following the arrest of the alleged Golden State Killer, moreover, law enforcement appetite to make similar uses of genealogical DNA

[5] See Bear Brook: Chameleon, N.H. Public Radio (Nov. 7, 2018) (downloaded using iTunes) (describing the advent of using genetic genealogy to generate leads for police investigation beginning at five minutes).

[6] See Oreskes et al., supra note 1.

[7] See Michael Balsamo, Genetic Website Subpoenaed in California Serial Killer Probe, AP News (May 1, 2018), https://www.apnews.com/7ed5154e100e4ed2b1ac391d2faea203 [https://perma.cc/C92A-CDV8]; Oreskes et al., supra note 1.

[8] Balsamo, supra note 7; Oreskes et al., supra note 1.

[9] See Jim Mustian, New Orleans Filmmaker Cleared in Cold-Case Murder; False Positive Highlights Limitations of Familial DNA Searching, New Orleans Advoc. (Mar. 12, 2015), https://www.nola.com/news/article_d58a3d17-c89b-543f-8365-a2619719f6f0.html [https://perma.cc/XU9Z-Z2SQ]; see also Natalie Ram, DNA by the Entirety, 115 Colum. L. Rev. 873, 883 n.64 (2015) (discussing the Usry case).

[10] See Mustian, supra note 9.

[11] Id.

[12] Id.

[13] See Megan Cassidy, How Forensic Genealogy Led to an Arrest in the Phoenix 'Canal Killer' Case, Ariz. Repub. (Nov. 30, 2016), https://www.azcentral.com/story/news/local/phoenix/2016/11/30/how-forensic-genealogy-led-arrest-phoenix-canal-killer-case-bryan-patrick-miller-dna/94565410/ [https://perma.cc/3B96-BNME].

databases rapidly materialized. Within weeks, Parabon NanoLabs, a private company working with investigators, was commissioned to sequence and upload DNA from more than 100 other crime scenes to GEDmatch, in hopes of cracking more cold cases.[14] In the months since, investigators have relied on consumer genetics databases to generate suspects in more than forty other cases,[15] leading to dozens of arrests.[16]

Meanwhile, consumer genetic services have responded to law enforcement desire to use their resources to solve crimes in markedly different ways. Services, including 23andMe and Ancestry, have promised to guard user privacy against government access—and appear to be following through. 23andMe emphasized after the Golden State Killer arrest that "it's 'our policy to resist law enforcement inquiries to protect customer privacy.'"[17] Although 23andMe acknowledges that "[i]n certain circumstances, . . . 23andMe may be required by law to comply with a valid court order, subpoena, or search warrant for genetic or personal information,"

[14] See Julian Hattem, Investigators Say DNA Database Can Be Goldmine for Old Cases, AP News (June 16, 2018), https://www.apnews.com/96ee418316c343649df5d10d2a44c600 [https://perma.cc/J4HU-TJP6]. Although Parabon is a private entity, its conduct is properly attributable to the government. See, e.g., Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 614 (1989) ("Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government."). Law enforcement entities pay Parabon for its genealogical genetic sleuthing and make DNA extracted from crime scene evidence available for its analysis and use. See Frequently Asked Questions (FAQs) About Snapshot, Parabon NanoLabs, https://snapshot.parabon-nanolabs.com/faq [https://perma.cc/T5M5-JMN6] (last visited Aug. 13, 2019) (responding to "How does my agency order a Snapshot analysis?"). Parabon thus acts as an agent of law enforcement in carrying out this work.

[15] See Heather Murphy, Genealogy Sites Have Helped Identify Suspects. Now They've Helped Convict One, N.Y. Times (July 1, 2019), https://www.nytimes.com/2019/07/01/us/dna-genetic-genealogy-trial.html [https://perma.cc/RDN4-2RZC]; see also Megan Molteni, The Future of Crime-Fighting Is Family Tree Forensics, Wired (Dec. 26, 2018), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/ [https://perma.cc/A9RX-H6AF] (describing how use of GEDmatch led to over 20 arrests); Heather Murphy, How an Unlikely Family History Website Transformed Cold Case Investigations, N.Y. Times (Oct. 15, 2018), https://www.nytimes.com/2018/10/15/science/gedmatch-genealogy-cold-cases.html [https://perma.cc/K2PC-NPXB] (noting at least fifteen cases in which a GEDmatch DNA match "provided essential clues leading to a suspect in a murder or sexual assault case").

[16] See Natalie Ram, The U.S. May Soon Have a De Facto National DNA Database, Slate (Mar. 19, 2019), https://slate.com/technology/2019/03/national-dna-database-law-enforcement-genetic-genealogy.html [https://perma.cc/4T3P-3RNK].

[17] Keith Wagstaff, Suspected Serial Killer Caught After Relative Shares DNA with Genealogy Website, Mashable (Apr. 26, 2018), https://mashable.com/2018/04/26/golden-state-killer-joseph-james-deangelo-dna-ancestry-websites [https://perma.cc/CWG5-75FY].

the company asserts that it will "use all practical legal and administrative resources to resist requests from law enforcement, and we do not share customer data with any public databases, or with entities that may increase the risk of law enforcement access."[18] Ancestry similarly emphasizes that it "will not share your Genetic Information with law enforcement unless compelled by valid legal process."[19]

But other services have taken a more permissive approach to law enforcement access to user genetic data—even encouraging users to participate in their services because of their availability to law enforcement. Consider GEDmatch. Within weeks of learning that investigators had relied on GEDmatch, among others, in the Golden State Killer investigation that site's operators updated the GEDmatch user interface, terms of service, and privacy policy to welcome law enforcement, explaining that DNA may be uploaded to its platform if it was "obtained and authorized by law enforcement to . . . identify a perpetrator of a violent crime against another individual."[20] At the time, GEDmatch defined a "violent crime" to include only homicide and sexual assault.[21]

This iteration of GEDmatch's privacy practices, however, lasted less than a year. In late 2018, the GEDmatch operators authorized law enforcement to use its database to investigate an aggravated assault.[22] In May 2019, when the public learned of this derogation from the site's own policies limiting law enforcement access to homicide and sexual assault crimes,[23] GEDmatch altered its stance to require existing users to opt-in to law enforcement use of their genetic data[24]—though new genetic

[18] 23andMe Guide for Law Enforcement, 23andMe, https://www.23andme.com/law-enforcement-guide/ [https://perma.cc/L83U-UX6D] (last visited Sept. 6, 2019).

[19] Ancestry Terms and Conditions, Ancestry (July 25, 2019), https://www.ancestry.com/-cs/legal/termsandconditions [https://perma.cc/FW23-C9MW].

[20] GEDmatch.com Terms of Service and Privacy Policy, GEDmatch (May 20, 2018) (on file with Virginia Law Review Association).

[21] Id.

[22] See Peter Aldhous, The Arrest of a Teen on an Assault Charge Has Sparked New Privacy Fears About DNA Sleuthing, BuzzFeed News (May 14, 2019), https://www.buzzfeednews.com/article/peteraldhous/genetic-genealogy-parabon-gedmatch-assault [https://perma.cc/U6UL-33UA].

[23] See id.

[24] See GEDmatch Tools for DNA and Genealogy Research, GEDmatch, https://www.gedmatch.com/select.php (last visited Sept. 10, 2019) (on file with Virginia Law Review Association) ("On May 18, GEDmatch changed its rules relating to matches with kits uploaded by representatives of Law Enforcement. All previously existing DNA kits in the GEDmatch database were set to 'opt-out' of these comparisons.").

profiles appear to be opted-in by default.[25] At the same time, GEDmatch expanded the range of permitted investigations to encompass "murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault."[26] GEDmatch has since actively encouraged users to opt in to law enforcement use,[27] and, by early July 2019, roughly 85,000 user genetic profiles had been made available for such use.[28]

Finally, in late January 2019, the public learned that FamilyTreeDNA, another large consumer genetics company, had also been working with the FBI for the last year to process and compare crime scene DNA to the genetic profiles in its database—without explicitly informing its users about this practice.[29] Indeed, all the while, FamilyTreeDNA held itself out as committed to user privacy, summarizing its privacy policy as a commitment that "[w]e won't share your DNA."[30] In March 2019, FamilyTreeDNA adopted a "law enforcement matching" option like the one now available at GEDmatch, except that all U.S.-based FamilyTreeDNA user data is available to law enforcement by default.[31] New and existing users must affirmatively opt out of law enforcement access.[32]

[25] See GEDmatch Raw DNA Upload Utility, GEDmatch, https://www.gedmatch.com/v_upload1.phpnf (last visited Aug. 28, 2019) (pre-selecting the radio dial to "opt-in" to law enforcement access for new uploads of genetic data) (on file with Virginia Law Review Association).

[26] GEDmatch.com Terms of Service and Privacy Policy, GEDmatch (May 18, 2019), https://www.gedmatch.com/tos.htm [https://perma.cc/87WU-9JHW].

[27] See GEDmatch Tools for DNA and Genealogy Research, GEDmatch, https://www.gedmatch.com/select.php (last visited Aug. 28, 2019).

[28] See Hautala, supra note 3.

[29] See Salvador Hernandez, One of the Biggest At-Home DNA Testing Companies Is Working with the FBI, Buzzfeed (Jan. 31, 2019), https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy [https://perma.cc/4SXY-YB29]; Amy Dockser Marcus, Customers Handed Over Their DNA. The Company Let the FBI Take a Look., Wall St. J. (Aug. 22, 2019), https://www.wsj.com/articles/customers-handed-over-their-dna-the-company-let-the-fbi-take-a-look-11566491162 [https://perma.cc/-5NFN-KKAZ]. Law enforcement are not able to view the hundreds of thousands of individual SNPs in a matching user's genetic profile. Rather, "[w]hen there is a genetic match in the FamilyTreeDNA database, the FBI sees what a regular customer sees: the name of the person if the customer has provided it, the amount of DNA that is shared in common, and contact information if the customer lists it." Id.

[30] See FamilyTreeDNA, https://www.FamilyTreeDNA.com (last visited Sept. 10, 2019).

[31] See We Are Updating Our Terms of Service and Privacy Statement Regarding Law Enforcement Matching Preferences, FamilyTreeDNA (Mar. 12, 2019) [hereinafter FamilyTreeDNA March 2019 Updates], https://mailchi.mp/familytreedna/updates-to-our-terms-of-service-and-privacy-policy-march19?e=dfef197239 [https://perma.cc/AL72-8WFF].

[32] Id.

FamilyTreeDNA has also doubled down on law enforcement collaboration, making such efforts the subject of an advertisement.[33]

These services are growing rapidly, encompassing an ever-greater proportion of the U.S. population—directly and indirectly through familial genetic association.[34] GEDmatch is home to more than a million users' genetic data.[35] FamilyTreeDNA maintains genetic data from more than two million users.[36] 23andMe has at least five million genetic profiles in its database.[37] Ancestry claims more than ten million.[38] In all, one report estimates that more than twenty-six million people have already made use

[33] See Sarah Zhang, A DNA Company Wants You to Help Catch Criminals, Atlantic (Mar. 29, 2019), https://www.theatlantic.com/science/archive/2019/03/a-dna-company-wants-your-dna-to-catch-criminals/586120/ [https://perma.cc/SV76-6HXV].

[34] See Yaniv Erlich et al., Identity Inference of Genomic Data Using Long-Range Familial Searches, 362 Sci. 690, 690 (2018) (demonstrating through statistical modeling that more than sixty percent of individuals of European-descent may be findable through a genealogical genetic database of as few as 1.3 million people).

[35] See Hautala, supra note 3 ("Users have opted back in about 85,000 of the site's more than 1 million kits so far."); Dan Vergano, Here's How Amateur Sleuths and Police Investigators Used DNA Websites to Find the Golden State Killer, BuzzFeed News (Apr. 27, 2018), https://www.buzzfeednews.com/article/danvergano/gedmatch-serial-killer-dna#.hoywmeX-RmJ [https://perma.cc/8ZWF-FFTG] ("While GEDmatch had perhaps 100,000 genomes in 2014 . . . it now has a million and counting, making it more powerful every day.").

[36] See FamilyTreeDNA supra note 30 (under "Frequently Asked Questions," under "Who is FamilyTreeDNA," stating, "Over 2 million people have tested with FamilyTreeDNA, resulting in the most comprehensive DNA matching database in the industry"); see also Antonio Regalado, More than 26 Million People Have Taken an At-Home Ancestry Test, MIT Tech. Rev. (Feb. 11, 2019), https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/ [https://perma.cc/G5CK-3UR2] ("Gene By Gene, a Houston company, told us its Family Tree DNA ancestry database has about 2 million people in it, but half underwent earlier, less comprehensive forms of testing, and about 20% of the profiles it holds are uploads of data generated by other companies.")

[37] See Megan Molteni, 23andMe's Pharma Deals Have Been the Plan All Along, Wired (Aug. 3, 2018), https://www.wired.com/story/23andme-glaxosmithkline-pharma-deal/ [https://perma.cc/DR8Y-RNCT] ("Since the launch of its DNA testing service in 2007, genomics giant 23andMe has convinced more than 5 million people to fill a plastic tube with half a teaspoon of saliva.") The true number of U.S.-based users may be far higher, however. See Regalado, supra note 36 ("Although 23andMe has not publicly released a figure recently, a person familiar with the company's figures and market data said it has now tested more than 9 million people.").

[38] See Ancestry, AncestryDNA, https://www.ancestry.com/dna/ [https://perma.cc/W2G4-JQZB] (last visited Aug. 20, 2019) ("More than 10 million people have uncovered something new about themselves.").

of a consumer genetic service.[39] These platforms are also examining a growing range of genetic data in providing their services.[40]

Might these companies' differing approaches to user privacy vis-a-vis law enforcement affect the substantive privacy rights of those users, as a constitutional matter? Until recently, as a matter of Fourth Amendment doctrine, the answer was plainly no.[41] Under the so-called third-party doctrine, the mere act of voluntarily sharing information with a third party, like a genealogical DNA service provider, rendered it beyond the protections of the Fourth Amendment's prohibition of unreasonable searches and seizures.[42] Privacy practices were relevant only insofar as they might inform users that their data was being collected at all, in which case no expectation of privacy could follow.[43]

[39] Regalado, supra note 36.

[40] See Find Out What Your DNA Says About Your Health, Traits and Ancestry, 23andMe, [hereinafter About 23andMe Ancestry+Health DNA Service], https://www.23andme.com/dna-health-ancestry/ [https://perma.cc/5FT5-6QQ4] (last visited Aug. 13, 2019) (identifying a growing number of "Genetic Health Risk reports," "Ancestry reports," "Wellness reports," "Carrier Status reports," and "Trait reports"); Discover Your Origins, Historical Details, and DNA Matches, Ancestry, https://www.ancestry.com/cs/offers/traits [https://perma.cc/XDK5-H5UU] (last visited July 17, 2019) (advertising AncestryDNA Traits, which will "[u]nlock personal traits your genes could influence—from the things you see, like eye color, to things you can't, like how you taste bitter flavors").

[41] This Article focuses on constitutional limitations on police access to digital data, particularly genetic data. It does not consider the ways in which service providers and other intermediaries may erect barriers of other kinds. 23andMe and Ancestry, for instance, have created a practical barrier to police use of their genealogical genetic data, by requiring a sizeable saliva sample for analysis. See Providing Your Saliva Sample, 23andMe, https://customercare.23andme.com/hc/en-us/articles/202904530 [https://perma.cc/TUW6-WXEE] (last visited Oct. 2, 2019) ("The recommended volume of saliva to provide is about 2 mL, or about 1/2 teaspoon."); Taking an AncestryDNA Test, Ancestry, https://support.ancestry.com/s/article/US-Taking-a-DNA-Test (last visited Oct. 2, 2019) (providing advice for what to do "[i]f you can't produce enough saliva in one try"). This requirement may impact the ability of law enforcement investigators to compare a crime scene genetic sample to genetic profiles housed by these services, but merely as a practical matter, rather than a legal matter. This practical limitation would disappear if investigators develop technology to synthesize saliva from a genetic sample. See Andrew Pollack, DNA Evidence Can Be Fabricated, Scientists Show, N.Y. Times (Aug. 17, 2009), https://www.nytimes.com/2009/08/18/science/18dna.html [https://perma.cc/B2FG-L4HE]. Nonetheless, the legal considerations considered here would remain.

[42] See William Baude & James Y. Stern, The Positive Law Model of the Fourth Amendment, 129 Harv. L. Rev. 1821, 1871 (2016) ("It is black-letter law under *Katz* that people don't have any Fourth Amendment protection for information given to a third party."); Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (describing the "third-party doctrine").

[43] See infra Section III.A.

But in *Carpenter v. United States*, the Supreme Court appears to have upended, or at least softened, that previously categorical rule. In *Carpenter*, the Court held that government access to a week's worth of a user's historical cell phone location data—data that is compiled and held by cell phone companies—is nonetheless data in which the user maintains an expectation of privacy.[44] Such access thus amounts to a search subject to the Fourth Amendment, and typically requires a warrant.[45] Although the *Carpenter* Court insisted that its opinion is narrow,[46] its language and reasoning will inevitably reinvigorate user privacy in many domains. Indeed, this is already happening.[47] In particular, the Court's solicitude for the privacy that can inhere in sensitive, personal data, even when that data is in another's possession, invites elaboration about what other kinds of data are sufficiently sensitive to merit closer analysis and what circumstances influence whether privacy can reasonably be expected.

This Article is the first in a pair of works that interrogate the impact of *Carpenter* for investigations like the ones in the Golden State Killer case. More specifically, this Article evaluates the impact of *Carpenter* for individuals whose own cells have been analyzed and whose genetic data is stored in a third-party repository or database. After *Carpenter*, the question is what, if any, authority these platforms have, as a constitutional matter, to facilitate—or prevent—law enforcement access to the millions of genetic profiles that they maintain. This Article provides an answer, and in doing so makes three contributions to the literature.

First, the Article argues that, after *Carpenter*, genetic data is the kind of sensitive, personal information in which individuals may generally retain an expectation of privacy against government surveillance, even when that information is in third-party hands. Part I joins a burgeoning scholarship in identifying the key aspects of digital data, its aggregation, and its use by law enforcement that undergird the Court's analysis in *Carpenter*. Part II demonstrates that these same features are present or growing in the context of consumer genetic data.

Second, Part III considers whether this leaves any space for consumer genetic platforms in mediating police access to their resources,

[44] See *Carpenter*, 138 S. Ct. at 2219, 2220.

[45] See id. at 2223.

[46] See id. at 2220 ("Our decision today is a narrow one.").

[47] See Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018) (applying *Carpenter* to conclude that government access to smart electric meter data constitutes a Fourth Amendment search).

concluding that these platforms may yet harbor some authority to expose the genetic resources they hold to law enforcement investigation—but only in instances in which those platforms obtain knowing and voluntary consent for such exposure from their users.

Third, Part IV takes stock of the range and change in privacy practices and disclosures in place at a variety of consumer genetic platforms, including 23andMe, Ancestry, GEDmatch, and FamilyTreeDNA. In so doing, it charts how these platforms have attempted either to reinforce existing expectations of privacy in user genetic data or to facilitate consent to law enforcement access to that data, with varying degrees of success. As several of these privacy practices have shifted rapidly, over even the past year, conclusions about whether any platform has achieved valid consent for law enforcement access is necessarily tentative at best. Nonetheless, in identifying disclosures and consent that courts may, or should not, deem acceptable for facilitating law enforcement access, this Article seeks to provide guidance for future development in the privacy space.

A second, companion article takes up a related question of third-party genetic privacy after *Carpenter*—its impact on familial genetic identification.[48] This type of identification exploits one individual's genetic data to learn about or identify as a suspect a genetic relative whose cells are not directly within the scope of known individuals in a database. Where one individual's affirmative consent to share genetic data puts private data of another in view, it will not always be clear that the privacy of that second party has effectively been waived. Accordingly, the current Article sets issues of familial forensic identification to the side, assessing first the core question of how *Carpenter* applies to genetic data at all and what to make of divergent privacy practices in the consumer genetic marketplace in its wake.

I. CONSTRUCTING *CARPENTER*

Carpenter marks a sea change in Fourth Amendment analysis of privacy claims in digital data held in third-party hands, making viable a range of expectations of privacy that the law was ill-suited to recognize previously. But *Carpenter*'s assessment of expectations of privacy in cell phone location data did not emerge from thin air. Rather, it was both the culmination of a gradual skepticism about the so-called third-party

[48] See Natalie Ram, Genetic Genealogy and the Problem of Familial Forensic Identification (unpublished manuscript) (on file with author).

doctrine and how that doctrine should apply in the digital age, and a concrete first step in reconfiguring that relationship. This Part unpacks the *Carpenter* decision, identifying the key features of its analysis and describing its core test going forward. Section I.A sets *Carpenter* in its historical and recent context. Section I.B describes the *Carpenter* decision itself and delineates the key aspects of *Carpenter*'s likely "test" going forward.

A. Contextualizing Carpenter

The Fourth Amendment enshrines "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[49] Ordinarily, police must obtain a warrant, supported by probable cause, before performing a search that is intended to discover criminal conduct.[50] Since *Katz v. United States*, the Supreme Court, in interpreting the Fourth Amendment, has explained that the Amendment "protects people, not places."[51] To determine whether a "search" has occurred, and thus whether constitutional scrutiny is appropriate, courts have asked whether the place, thing, or information that the police seek to examine is one in which an individual has an "expectation of privacy . . . that society is prepared to recognize as reasonable."[52] Where that is so, the Court has held that "official intrusion into that private sphere generally qualifies as a search and requires a warrant

[49] U.S. Const., amend. IV.

[50] See *Carpenter*, 138 S. Ct. at 2221 ("Although the ultimate measure of the constitutionality of a governmental search is *reasonableness*, our cases establish that warrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing." (internal quotation marks omitted) (emphasis added)).

[51] Katz v. United States, 389 U.S. 347, 351 (1967).

[52] *Carpenter*, 138 S. Ct. at 2213 (internal quotation marks omitted); *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Prior to *Katz*, the Supreme Court's analysis of Fourth Amendment searches focused instead on the concept of physical property. In *Olmstead v. United States*, for instance, the Court held that the Fourth Amendment did not apply to a government wiretap of a phone line because the wiretap did not necessitate a physical trespass. 277 U.S. 438, 464–66 (1928). *Katz* famously repudiated *Olmstead*'s holding and added the "expectation of privacy" test to the Court's Fourth Amendment tool kit. The Court has recently reinvigorated the use of trespass concepts in evaluating whether a search or seizure has occurred. See Florida v. Jardines, 569 U.S. 1, 11 (2013); United States v. Jones, 565 U.S. 400, 405–08 (2012); see also *Carpenter*, 138 S. Ct. at 2267–71 (Gorsuch, J., dissenting) (arguing that the Court should largely reject *Katz*'s "expectations of privacy" test in favor of a positive law inquiry). But a majority of the Court continues to subscribe to *Katz*'s "expectations of privacy" framework.

supported by probable cause."[53] Although scholars have criticized the "expectations of privacy" inquiry,[54] the Supreme Court has consistently reaffirmed its adherence to that approach—including most recently in *Carpenter v. United States*.[55]

In a pair of cases in the 1970s, the Court elaborated on how this "expectation of privacy" test should apply when an individual shares information with a third party from whom the government subsequently obtains that information. In *United States v. Miller*, the Supreme Court confronted how *Katz* should apply to data held in third-party hands.[56] *Miller* involved government acquisition of bank records, which the bank was required to maintain as a matter of federal law.[57] The Court concluded that an individual could have no legitimate expectation of privacy in his bank records, and so the government could obtain them by subpoena of the bank free from the strictures of the Fourth Amendment.[58] In *Smith v. Maryland*, the Supreme Court went on to hold that the use of a pen register at the telephone company office to record telephone numbers dialed did not constitute a "search" subject to the Fourth Amendment either.[59]

[53] *Carpenter*, 138 S. Ct. at 2213. There are a number of exceptions to the warrant requirement. For example, a warrant is not required where police undertake a search for reasons other than uncovering evidence of criminal conduct. See Indianapolis v. Edmond, 531 U.S. 32, 37 (2000). A warrant also is not required where police confront exigent circumstances, see Mitchell v. Wisconsin, No. 18-6210, slip op. at 8 (U.S. S. Ct. June 27, 2019); Warden v. Hayden, 387 U.S. 294, 298–99 (1967) (citing McDonald v. United States, 335 U.S. 451, 456 (1948)); or for searches incident to an arrest, see Chimel v. California, 395 U.S. 752, 762–63 (1969), among others.

[54] See, e.g., Matthew Tokson, Knowledge and Fourth Amendment Privacy, 111 Nw. U. L. Rev. 139, 147 (2016) ("The *Katz* test is simple and concise on the page. But in application it is frequently puzzling, and its true nature remains something of a mystery."); Orin S. Kerr, An Equilibrium-Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev. 476, 533–34 (2011); see also *Carpenter*, 138 S. Ct. at 2244 (Thomas, J., dissenting) ("Jurists and commentators tasked with deciphering our jurisprudence have described the *Katz* regime as 'an unpredictable jumble,' 'a mass of contradictions and obscurities,' 'all over the map,' 'riddled with inconsistency and incoherence,' 'a series of inconsistent and bizarre results that [the Court] has left entirely undefended,' 'unstable,' 'chameleon-like,' 'notoriously unhelpful,' 'a conclusion rather than a starting point for analysis,' 'distressingly unmanageable,' 'a dismal failure,' 'flawed to the core,' 'unadorned fiat,' and 'inspired by the kind of logic that produced Rube Goldberg's bizarre contraptions.'").

[55] 138 S. Ct. at 2213–14 (explaining and defending the *Katz* approach). But see id. at 2214 n.1 (observing that "[n]either party has asked the Court to reconsider *Katz* in this case").

[56] 425 U.S. 435, 442 (1976).

[57] Id. at 441.

[58] Id. at 440.

[59] 442 U.S. 735, 745–46 (1979).

In both cases, the Court explained that the information the government sought to access was not really private or confidential at all. Bank records memorializing checks and deposit slips were "not confidential communications but negotiable instruments to be used in commercial transactions."[60] Similarly, a pen register has only "limited capabilities," such that the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial."[61] Moreover, the Court reasoned that the defendants had "voluntarily conveyed" the information at issue to a third party, and in so doing "assumed the risk" that the company's records "would be divulged to police."[62]

In the decades following *Miller* and *Smith*, courts typically read these decisions as establishing a categorical rule: "if you share information, you do not have an expectation of privacy in it."[63] The categorical nature of this "third-party doctrine" was not without basis. After all, *Smith* had declared that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[64] *Miller*, meanwhile, demonstrated that this was true "even if the information is revealed on the assumption that it will be used only for a limited purpose."[65] Thus, from the 1970s until 2018, courts largely held that individuals had no Fourth Amendment expectation of privacy in any data shared with a third party, no matter how sensitive that data might otherwise appear to be.[66]

To be sure, there were occasional and narrow limitations to this rule. In *Ferguson v. City of Charleston*, for instance, the Supreme Court held that it violated the Fourth Amendment for hospital personnel to analyze patient urine samples with the intent to convey information about drug

[60] *Miller*, 425 U.S. at 442.

[61] *Smith*, 442 U.S. at 742.

[62] Id. at 744–45; see also *Miller*, 425 U.S. at 442–43 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

[63] Margot E. Kaminski, Response, *Carpenter v. United States:* Big Data Is Different, Geo. Wash. L. Rev.: On the Docket (July 2, 2018), https://www.gwlr.org/carpenter-v-united-states-big-data-is-different [https://perma.cc/6HT8-6JTW] (describing this rule as a "central truism of U.S. privacy law" until *Carpenter*); see also Baude & Stern, supra note 42, at 1871 ("It is black-letter law under *Katz* that people don't have any Fourth Amendment protection for information given to a third party.").

[64] *Smith*, 442 U.S. at 743–44.

[65] *Miller*, 425 U.S. at 443.

[66] See, e.g., Note, If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine, 130 Harv. L. Rev. 1924, 1930 (2017) ("Over the thirty-three years following *Smith*, courts applied the third party doctrine with relative consistency.").

use to the police.[67] As the dissenting Justices noted in *Ferguson*, such a holding fit poorly with a rule that "material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain."[68] But *Ferguson* confined itself to the special circumstances of a physician-patient relationship and emphasized that hospital personnel in that case were themselves public employees who had undertaken urine analysis with crime detection in mind.[69]

In recent years, however, some members of the Court began to express growing unease about the appropriateness of a categorical third-party doctrine. In *United States v. Jones*, the Court considered whether the government ran afoul of the Fourth Amendment when it attached a GPS device to Jones's vehicle and tracked his location for an extended period of time.[70] All nine members of the Court agreed that this government conduct violated the Fourth Amendment.[71] In a concurring opinion, however, Justice Sotomayor explained that, in a future case, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," as that "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."[72] The Court did not reach this reconsideration in *Jones*, since the location data there had been obtained from a government-placed device, rather than from a third-party service provider.[73]

The Court further elaborated on the expectations of privacy that might attach to digital data in *Riley v. California*, holding that police examination of the contents of a cell phone constitutes a Fourth Amendment search, and that the warrant exception for searches incident to arrest does not extend to immunize such an examination.[74] The Court explained that "[c]ell phones differ in both a quantitative and a qualitative sense from

[67] 532 U.S. 67, 86 (2001); see also Kiel Brennan-Marquez, Fourth Amendment Fiduciaries, 84 Fordham L. Rev. 611, 628 (2015) (arguing that *Ferguson* is an exception to the third-party doctrine that should be grounded in the physician-patient fiduciary relationship).

[68] 532 U.S. at 95 (Scalia, J., dissenting).

[69] See id. at 78, 83–84.

[70] 565 U.S. 400, 402–03 (2012).

[71] Id. at 404, 413; id. at 413–14 (Sotomayor, J., concurring); id. at 431 (Alito, J., concurring in judgment).

[72] Id. at 417 (Sotomayor, J., concurring).

[73] Id. at 403.

[74] 134 S. Ct. 2473, 2485 (2014).

other objects that might be kept on an arrestee's person."[75] Cell phones contain a trove of sensitive data, including internet search and browsing history, historical location information, and apps that can reveal a person's interests or otherwise detailed information about them.[76] Perhaps most significantly, the Court did not appear to consider the remote storage of much of this sensitive information to undermine any Fourth Amendment interests.[77]

B. Framing the Carpenter *Test*

Carpenter asked the question that Justice Sotomayor presaged in her *Jones* concurrence: if comprehensive location information is sensitive and ordinarily subject to an expectation of privacy, does sharing that information with a service provider necessarily negate that expectation?[78] In *Carpenter*, police investigating a string of robberies had applied for and received a court order under the Stored Communications Act compelling Carpenter's cell phone providers, Sprint and MetroPCS, to turn over several days worth of Carpenter's historical cell site location information.[79] The Stored Communications Act permits police to gain access to stored electronic records like these that are "relevant and material to an ongoing investigation."[80] As the Court observed, such a standard "falls well short of the probable cause required for a warrant."[81] Nonetheless, applying the well-settled third-party doctrine, the district court and court of appeals held that Carpenter had "lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers."[82]

The Supreme Court disagreed. The Court explained that *Carpenter* arises at the intersection of two lines of doctrine: the first about the sensitive information implicated by location data, as discussed in *Jones* and *Riley*, and the second involving the third-party doctrine.[83] Guided by "historical understandings" surrounding the Fourth Amendment, the Court

[75] Id. at 2489.
[76] Id. at 2490.
[77] Id. at 2491.
[78] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).
[79] Id. at 2212.
[80] 18 U.S.C. § 2703(d) (2012).
[81] *Carpenter*, 138 S. Ct. at 2221.
[82] Id. at 2213.
[83] Id. at 2214–16.

explained that *Katz*'s expectations of privacy test must reflect the Fourth Amendment's goals "to secure the privacies of life against arbitrary power" and "to place obstacles in the way of a too permeating police surveillance."[84] And in view of these principles, the Court declined to "extend *Smith* and *Miller*" to cover historical cell site location information.[85]

The Court explained that *Smith* and *Miller* did not announce a categorical rule after all. Where sensitive, personal information is at stake, sharing that information with a third party does not necessarily undermine an otherwise reasonable expectation of privacy.[86] The Court determined that shared historical cell phone location information is quite unlike the bank records and phone numbers at issue in *Miller* and *Smith*.[87] First, the data at issue—location information on the one hand, and bank records and phone numbers on the other—are crucially different. Historical location information is highly sensitive, personal, and pervasive, while *Miller* and *Smith* had held that bank records were non-private "negotiable instruments" or that pen registers had "limited capabilities."[88] An individual typically has an expectation of privacy in the former, but not the latter, regardless of whether a third party is involved.

Second, the principle of "voluntary exposure" underlying the third-party doctrine is a poor fit for cell phone location information.[89] Cell phones are too ubiquitous in daily life to be truly a "voluntary" part of life, and their transmission of location information is an automatic, largely invisible facet of a phone's operation.[90]

In sum, the Court explicitly identified three key factors informing its conclusion that individuals retain an expectation of privacy in their location information, despite sharing that information with their cell phone providers: first, "the deeply revealing nature" of the information sought; second, "its depth, breadth, and comprehensive reach"; and third, "the inescapable and automatic nature of its collection."[91] In addition, the Court recognized a fourth such factor, emphasizing that a more limited third-party doctrine is particularly important where the government can make use of otherwise sensitive data held by a third-party in "remarkably easy,

[84] Id. at 2214 (internal quotation marks omitted).
[85] Id. at 2217.
[86] Id. at 2220.
[87] Id. at 2219.
[88] Id. at 2219–20.
[89] Id. at 2220.
[90] Id.
[91] Id. at 2223.

cheap, and efficient [ways,] compared to traditional investigative tools," such as "[w]ith just the click of a button."[92]

The Court thus refused to allow the third-party doctrine to swallow the Fourth Amendment in the digital age. Where an individual has an otherwise reasonable expectation of privacy in her data, merely sharing that data with a third party does not, in itself, negate that expectation.

Having concluded that police access to an individual's historical cell phone location information contravenes a reasonable expectation of privacy, and thus constitutes a Fourth Amendment search, the Court went on to conclude that such searches will ordinarily require a warrant.[93] Although "reasonableness" is the "ultimate measure of the constitutionality of a governmental search," the Court emphasized that, "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."[94] The Court found that court orders issued pursuant to the Stored Communications Act were insufficient to substitute for a warrant.[95]

Carpenter insists that its holding is "narrow,"[96] but the implications of its more limited construction of the third-party doctrine are likely to have broader impact. To be sure, the Court expressly reserves judgment about other technologies, including "real-time [cell phone location information] or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)," and purports to leave unquestioned "conventional surveillance techniques and tools, such as security cameras."[97] But the strongest versions of the third-party doctrine are now weakened in light of *Carpenter*'s conclusion that "the fact that . . . information is gathered by a third party does not make it any

[92] Id. at 2218; see also Paul Ohm, The Many Revolutions of *Carpenter*, 32 Harv. J.L. & Tech. 357, 369–78 (2019) (identifying and explaining these four factors as *Carpenter*'s "test"). Other scholars, including Orin Kerr and Matthew Tokson, have identified similar, though not entirely overlapping, factors in defining the relevant "test" after *Carpenter*. See Orin Kerr, Implementing *Carpenter* 20, 22 (Dec. 19, 2018) (unpublished manuscript), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257 (arguing that *Carpenter* will control digital records "created without meaningful voluntary choice" that "tend to reveal 'the privacies of life'"); Matthew Tokson, The Emerging Principles of Fourth Amendment Privacy, 88 Geo. Wash. L. Rev. (forthcoming 2020) (manuscript at 12–26), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3425321 (identifying "intimacy," "amount," and "cost" as the relevant principles).

[93] *Carpenter*, 138 S. Ct. at 2221.

[94] Id. (internal quotation marks omitted).

[95] Id.

[96] Id. at 2220.

[97] Id.

less deserving of Fourth Amendment protection."[98] Indeed, lower courts have already applied *Carpenter*'s reasoning to technologies and data distinct from cell phones and location information.[99]

II. ESTABLISHING EXPECTATIONS IN GENETIC DATA

Before delving into the ways in which platform privacy practices may affect Fourth Amendment expectations of privacy in genetic data, this Part first analyzes the quality and type of data revealed through genetic analysis. Section II.A first explains how the genetic data compiled or stored by consumer genetic services is like, and importantly unlike, the genetic data already stored in official law enforcement-related genetic databases. Section II.B demonstrates that genetic information is precisely the kind of data to which Fourth Amendment expectations of privacy ordinarily ought to attach, even when that data is shared with a third-party service provider.

A. Understanding Genetic Databases

Investigative searches of DNA databases have been a well-accepted law enforcement technique since the early 1990s.[100] All fifty states, the District of Columbia, and a variety of federal agencies collect, store, and share genetic information for law enforcement purposes through a central database known as the Combined DNA Index System ("CODIS").[101] Pursuant to federal law, local, state, and federal forensic DNA laboratories may enter lawfully obtained genetic profiles into the CODIS "offender" database, while DNA profiles developed from crime scene evidence are stored in a separate CODIS index.[102] As of July 2019, the CODIS offender

[98] Id. at 2223.

[99] See Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018) (rejecting the third-party doctrine as applied to government access to smart electric meter data and explaining that, even if a third party were involved, *Carpenter*'s reasoning would render government access a Fourth Amendment search).

[100] See Natalie Ram, Fortuity and Forensic Familial Identification, 63 Stan. L. Rev. 751, 760 (2011).

[101] See Maryland v. King, 569 U.S. 435, 444–45 (2013).

[102] See 34 U.S.C. § 12592(a) (2012) (authorizing the Director of the FBI to "establish an index of . . . DNA identification records of . . . persons convicted of crimes," "persons who have been charged in an indictment or information with a crime," and "other persons whose DNA samples are collected under applicable legal authorities," as well as indices of "analyses of DNA samples recovered from crime scenes," "recovered from unidentified human remains," and "voluntarily contributed from relatives of missing persons").

database contains more than thirteen million offender profiles and an additional three million profiles from individuals arrested, but not yet convicted, of crimes.[103]

But the investigative use of non-law enforcement DNA databases, such as those compiled for genealogical purposes, is quite distinct from the traditional searches conducted in state-authorized databases. Most significantly, the purpose for which individuals provide their genetic data differs markedly. Individuals take part in direct-to-consumer genetic testing or genealogical genetic comparison to learn more about themselves—their ancestral origins, their previously unknown genetic relatives and related family history, and often their genetic predispositions to certain traits or diseases.[104] The motivations of individuals using platforms like 23andMe, GEDmatch, and others are largely separate from an interest in discovering unknown criminal relatives or aiding law enforcement in solving crimes.[105] To be sure, GEDmatch operator Curtis Rogers has reported that some users of his site have reached out to encourage continued law enforcement use of the GEDmatch database.[106] But until the arrest of the alleged Golden State Killer little more than a year ago, most users operated largely unaware of even the possibility of law enforcement use.[107]

Moreover, the scope, type, and intrusiveness of the data revealed in genealogical genetic sampling is far greater than that revealed in traditional law enforcement genetic analysis. The genetic data stored in non-law enforcement databases differs in the scope of individuals reachable through the database. Where CODIS is concerned, each participating jurisdiction is responsible for defining precisely which individuals are subject to DNA sampling for inclusion in CODIS, and each has done so by

[103] See CODIS – NDIS Statistics, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics [https://perma.cc/54YS-4TRX] (last visited Sept. 10, 2019).

[104] See, e.g., About 23andMe Ancestry+Health DNA Service, supra note 40 (describing the results 23andMe returns to users).

[105] See, e.g., Megan Molteni, The Key to Cracking Cold Cases Might Be Genealogy Sites, Wired (June 1, 2018), https://www.wired.com/story/police-will-crack-a-lot-more-cold-cases-with-dna [https://perma.cc/2QFB-FDAK] (reporting that CeCe Moore, Parabon's genealogical genetic expert, only began working with law enforcement after the Golden State Killer arrest, as she "never felt comfortable working with law enforcement while GEDmatch's users were unaware their data might be used that way").

[106] See id. (reporting that Rogers considered shuttering GEDmatch after the Golden State Killer arrest, but "after talking to users it became clear that people didn't want to lose an opportunity to contribute to a greater societal good").

[107] Id.

statute. Over time, the scope of includable individuals has expanded. The earliest DNA collection statutes limited their reach to convicted sex offenders.[108] Today, nearly all states and the federal government mandate DNA collection from all convicted felons,[109] most call for DNA collection for some misdemeanor convictions,[110] and more than half authorize DNA sampling of individuals arrested, but not convicted, of some crimes.[111] Despite this substantial growth in the scope and reach of CODIS, no jurisdiction to date has proposed the collection or search of DNA from ordinary members of the public for investigative use.[112] Yet, that is precisely what law enforcement use of genealogical genetic databases entails. These databases are populated with genetic data from millions of individuals with no known law enforcement connection.

The scope of information revealed by the data housed in non-forensic genetic databases is also markedly different from that of data housed in CODIS. CODIS profiles consist of forty data points drawn from twenty highly variable locations of the human chromosomes.[113] These data provide enough information to determine a probative match for similarly sequenced crime scene evidence—but they have been selected with an aim of revealing little else. These forty data points are located in noncoding

[108] See Ram, supra note 100, at 762; Tania Simoncelli, Dangerous Excursions: The Case Against Expanding Forensic DNA Databases to Innocent Persons, 34 J.L. Med. & Ethics 390, 390 (2006).

[109] See Convicted Offenders Required to Submit DNA Samples, Nat'l Conf. St. Legislatures (2013), http://www.ncsl.org/Documents/cj/ConvictedOffendersDNALaws.pdf [https://perma.cc/UM6N-RFPH].

[110] Id. ("42 states require the collection of samples for at least some misdemeanor convictions.").

[111] See DNA Arrestee Laws, Nat'l Conf. St. Legislatures (2013), http://www.ncsl.org/Documents/cj/ArresteeDNALaws.pdf [https://perma.cc/23LT-DG6M] ("Currently 30 states and the federal government" "authorize the analysis of DNA samples collected from individuals arrested or charged, but not convicted, of certain crimes.").

[112] Indeed, recent experience suggests that attempts to significantly expand the scope of official law enforcement databases to include individuals not associated with the criminal justice process will invite public outcry and failure. See Bree Burkitt, You May Soon Have to Give Your DNA to the State and Pay $250 for the Privilege, Ariz. Repub. (Feb. 19, 2019), https://www.azcentral.com/story/news/politics/arizona/2019/02/19/arizona-bill-would-create-massive-statewide-dna-database/2873930002/ [https://perma.cc/2R42-7PPS]; Bree Burkitt, Unrecognizable Version of DNA Bill Advances, Focuses on Rape Kits, Ariz. Repub. (Feb. 20, 2019), https://www.azcentral.com/story/news/politics/legislature/2019/02/20/arizona-dna-database-legislation-new-version-senate-bill-advances-rape-kit/2918578002/ [https://perma.cc/5Z8L-BGTD].

[113] See Combined DNA Index System (CODIS), FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis [https://perma.cc/8Q4C-SGZX] (last visited Sept. 10, 2019) (identifying the twenty CODIS loci used to created offender profiles).

DNA, which means the DNA involved does not code for proteins.[114] Legislatures and courts have long believed that noncoding DNA is relatively uninformative, and therefore only a minimal invasion of privacy.[115]

Genetic data compiled for other uses, by contrast, is far broader and more information-rich. Genealogical DNA profiles, like the ones used to crack the Golden State Killer case, consist of hundreds of thousands of DNA data points, strewn across the human chromosomes.[116] Indeed, companies like 23andMe, as well as platforms like GEDmatch that make secondary use of data produced by these companies, typically examine "600,000 variations of individual DNA letters, known as SNPs (pronounced 'snips') for single nucleotide polymorphisms."[117] Ancestry has claimed that its testing, like CODIS, is limited to non-coding portions of the human genome.[118] But the same service has also acknowledged that the data it sequences may be "associated with physical traits, such as hair color or traits associated with your health and wellness."[119]

At a minimum, genealogical DNA testing is highly revealing because it involves so much more genetic data than a CODIS profile—even if only noncoding information is used. As one advocate of using genealogical DNA data to help reidentify crime victims explained, "[t]he statistics you

[114] See Maryland v. King, 569 U.S. 435, 464–65 (2013).

[115] See, e.g., 12 R.I. Gen. Laws § 12-1.5-10(5) (2002) (forbidding use of DNA samples for purposes of "obtaining information about physical characteristics, traits or dispositions for disease"); Utah Code Ann. § 53-10-406(1) (LexisNexis 2015) (requiring bureau to "ensure that the DNA identification system does not provide information allowing prediction of genetic disease or predisposition to illness"); *King*, 569 U.S. at 464–65 (holding that "the processing of respondent's DNA sample's 13 CODIS loci did not intrude on respondent's privacy in a way that would make his DNA identification unconstitutional" because "the CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee," and observing that, "[i]f in the future police analyze samples to determine, for instance, an arrestee's predisposition for a particular disease or other hereditary factors not relevant to identity, that case would present additional privacy concerns not present here"). But see infra note 140 and accompanying text.

[116] See Tina Hesman Saey, New Genetic Sleuthing Tools Helped Track Down the Golden State Killer Suspect, Sci. News (Apr. 29, 2018), https://www.sciencenews.org/article/golden-state-killer-suspect-dna-genetics-genealogy [https://perma.cc/TH3C-EJW4].

[117] Id.

[118] See DNA Glossary of Terms, Ancestry, https://support.ancestry.com/s/article/DNA-Glossary-of-Terms-1460090079080 (last visited Aug. 28, 2019) ("Ancestry only tests the non-coding DNA regions of your DNA, since these are the regions containing information about your heritage.").

[119] See Your Privacy, Ancestry, https://www.ancestry.com/cs/legal/privacystatement [https://perma.cc/T4RY-8EE5] (last visited July 17, 2019) (describing "Genetic Information" under "What Information Does Ancestry Collect From You?").

can do on 600,000 SNPs are so much more powerful than statistics you can do on 20 [CODIS loci]."[120] For instance, genealogical DNA profiles can more easily identify distant genetic relatives. CODIS profiles, where state policy permits their use for familial identification purposes,[121] are largely limited to identifying first order relatives—parent-child or full sibling relationships.[122] As the Golden State Killer investigation demonstrates, genealogical genetic data can reveal second, third, or even more distant cousins.[123] Moreover, this data can more precisely "define the relationships between matches, showing that two people are first or third cousins, for instance," rather than just indicating a percentage of DNA matching.[124]

Nor does limiting genetic analysis to noncoding portions of the human genome actually serve as a sufficient privacy protection, either in CODIS or in genealogical genetic sequencing. As the foregoing makes clear, noncoding DNA can be highly informative about genetic relatedness, information that other forensic sciences typically cannot illuminate. Additionally, scientists are beginning to find that noncoding portions of DNA are not merely the "junk" they once thought. For example, researchers have uncovered links between noncoding regions of the genome and a host of genetic disorders, including certain neurodegenerative disorders and mental retardation syndromes.[125] The potential to detect such intimate information may complicate even this restricted analysis.

Moreover, in many instances, non-law enforcement uses of genetic data explicitly depend on analyzing coding DNA as well. Every one of

[120] Saey, supra note 116 (internal quotation marks omitted).

[121] See Ram, supra note 100, at 753.

[122] See Snapshot Kinship Inference, Parabon Nanolabs, https://snapshot.parabon-nanolabs.com/#kinship [https://perma.cc/VL3K-MC3F] (last visited Aug. 26, 2019) ("Traditional STR-based kinship analysis is limited to distinguishing parent/offspring relationships, often yielding inconclusive results for siblings or other second-degree relatives.").

[123] See id. (advertising that Parabon's Snapshot kinship analysis can "detect relatedness out to 9th-degree relationships—e.g., fourth cousins"); Jouvenal, supra note 3 (describing how investigators in the Golden State Killer case "used DNA recovered from a crime scene to find the killer's great-great-great grandparents, who lived in the early 1800s," and then traced the family tree forward to the present).

[124] Saey, supra note 116; see also Snapshot Kinship Inference, supra note 122 (advertising that, with Parabon's Snapshot service, "the precise degree of the relationship can be determined out to 6th-degree relatives (second cousins once removed)").

[125] See Ram, supra note 9, at 881; Karen Usdin, The Biological Effects of Simple Tandem Repeats: Lesson from the Repeat Expansion Diseases, 18 Genome Res. 1011, 1012–13 (2008) (concluding that many repeat expansion diseases "involve a repeat that is in a noncoding region of the gene" and providing examples).

23andMe's direct-to-consumer tests relies on coding DNA in full or in part. For its Ancestry service, 23andMe promises to "tell you how much of your DNA is derived from Neanderthals and how that compares to others. We can even point to specific Neanderthal DNA that is associated with traits that you might have—like height and back hair."[126] The linkage of genetic data to identifiable traits indicates that coding DNA, which helps determine traits, is likely at issue. Similarly, 23andMe's Health service includes reports for "Genetic Health Risks," "Wellness," "Carrier Status," and "Traits," each of which produces information about "genes"—coding DNA.[127] Ancestry's Traits service likewise depends on coding DNA to disclose information about users' "eye color" or "how you taste bitter flavors."[128]

Thus, genetic data stored in consumer genealogy databases is significantly different from the genetic data that courts have confronted in earlier cases. It is unrelated to the criminal justice system, and it can be far more revealing about the individual from whose cells the data derives, as well as about that individual's near and distant genetic relatives.

B. Individuals Retain an Expectation of Privacy in Genetic Data

As described above, the Supreme Court has continued to adhere to the principle that a Fourth Amendment "search" occurs, and thus constitutional scrutiny is appropriate, where the government intrudes on an individual's "expectation of privacy . . . that society is prepared to recognize as reasonable."[129] In *Carpenter*, the Court relied on roughly four factors to conclude that individuals retain an expectation of privacy in their cell phone location data, despite its third-party collection and storage: "the deeply revealing nature" of the information sought; the "depth, breadth, and comprehensive reach" of collections of such data; "the inescapable and automatic nature of its collection"; and the government's ability to make use of this data in "remarkably easy, cheap, and efficient [ways,] compared to traditional investigative tools," such as "[w]ith just the click

[126] DNA Ancestry, 23andMe, https://www.23andme.com/dna-ancestry/ [https://perma.cc/-MRT5-8PMZ] (last visited Aug. 8, 2019).

[127] About 23andMe Ancestry+Health DNA Service, supra note 40.

[128] Discover Your Origins, Historical Details, and DNA Matches, supra note 40 (advertising AncestryDNA Traits, which will "[u]nlock personal traits your genes could influence—from the things you see, like eye color, to things you can't, like how you taste bitter flavors").

[129] Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (internal quotation marks omitted); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

of a button."[130] Taking those factors in turn, this Section demonstrates that genetic data is precisely the kind of data in which individuals may ordinarily maintain expectations of privacy that are constitutionally significant—even when that data is shared with a third-party service provider.

1. Genetic Data Is Presumptively Private

Like the cell site location information at issue in *Carpenter*, genetic information is "deeply revealing,"[131] and so it is presumptively private in nature. The Supreme Court has already recognized that genetic data can carry with it reasonable expectations of privacy. In *Maryland v. King*, the Supreme Court considered whether subjecting an individual arrested, but not yet convicted, of a crime to genetic sampling, analysis, and inclusion in CODIS runs afoul of the Fourth Amendment.[132] In so doing, the Court considered the analysis of a compelled genetic sample to be a separate Fourth Amendment event from the acquisition of the sample itself.[133] The Court held that neither collection nor analysis of DNA is impermissible under the Fourth Amendment where an individual has been validly arrested for a serious offense.[134] Nonetheless, the separate consideration of genetic analysis indicates that genetic data carries with it an enduring privacy interest of constitutional magnitude.[135] That is, individuals retain a

[130] See *Carpenter*, 138 S. Ct. at 2218, 2223; see also Ohm, supra note 92 at 369–78 (identifying and explaining these four factors as *Carpenter*'s "test"); supra Section I.B.

[131] *Carpenter*, 138 S. Ct. at 2223; see also Ohm, supra note 92, at 384 (agreeing that genetic data satisfies *Carpenter*'s "deeply revealing nature factor").

[132] 569 U.S. 435, 441–42 (2013).

[133] Id. at 464–65.

[134] Id. at 465–66.

[135] Id. at 465 ("[O]nce respondent's DNA was lawfully collected the STR analysis of respondent's DNA pursuant to CODIS procedures did not amount to a significant invasion of privacy that would render the DNA identification impermissible under the Fourth Amendment."). Several courts of appeals have similarly discussed genetic analysis as a "search" separate from the collection of genetic material. See, e.g., United States v. Davis, 690 F.3d 226, 242–51 (4th Cir. 2012) (holding that police did not commit a Fourth Amendment violation in obtaining and using a crime victim's clothing in a subsequent criminal investigation, but that "the extraction and initial testing of Davis' [DNA] profile [from those clothes] was an unreasonable Fourth Amendment search"); United States v. Mitchell, 652 F.3d 387, 407 (3d Cir. 2011) (recognizing "processing of the DNA sample and creation of the DNA profile for CODIS" is a search with "potential to infringe upon privacy interests"); United States v. Amerson, 483 F.3d 73, 85 (2d Cir. 2007) (reiterating "'analysis and maintenance of [offenders'] information' in CODIS, the federal database is, in itself, a significant intrusion," which constitutes "a second and potentially much more serious invasion of privacy" (alteration in original) (quoting Nicholas v. Goord, 430 F.3d 652, 670 (2d Cir. 2005))); United States v. Sczubelek, 402 F.3d 175, 182 (3d Cir. 2005) ("'The ensuing chemical analysis of the sample

constitutionally significant "expectation of privacy . . . that society is prepared to recognize as reasonable"[136] not merely in their physical cells, but also in the genetic information those cells contain.

That expectation of privacy is particularly acute when the genetic data at issue includes more than merely the circumscribed data points used to compile a CODIS profile. In *King*, the Supreme Court explicitly reserved the question of whether the Fourth Amendment proscribes law enforcement access to genetic analysis related to, "for instance, an arrestee's predisposition for a particular disease or other hereditary factors not relevant to identity."[137] Genetic data that can reveal more than simply an individual's identity "would present additional privacy concerns."[138]

Yet that is precisely the kind of data stored in many non-law enforcement genetic repositories. As described above, companies like 23andMe utilize coding DNA to deliver each of their products, including those for genealogical research.[139] Moreover, scientists are discovering that even non-coding DNA is more revealing than previously believed.[140] And the use of hundreds of thousands of DNA data points, rather than merely forty, makes genealogical genetic analysis far more searching than the traditional forensic analysis that the Supreme Court faced in *King*.[141]

Other sources of law confirm that genetic data is sensitive, personal, and largely private. More than thirty states have enacted measures providing some protection for genetic information.[142] Although these laws differ substantially in their scope and exceptions, this volume of legislation indicates a widespread understanding that genetic data is, and ought to be, private.

---

to obtain physiological data' is also a search covered by the Fourth Amendment." (quoting Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 616 (1989))).

[136] *Carpenter*, 138 S. Ct. at 2213 (internal quotation marks omitted).

[137] *King*, 569 U.S. at 464–65.

[138] Id. at 465.

[139] See supra text accompanying notes 126–127.

[140] See Ram, supra note 9, at 881.

[141] Compare Saey, supra note 116 (reporting that genealogical DNA services typically analyze "600,000 variations of individual DNA letters, known as SNPs (pronounced 'snips') for single nucleotide polymorphisms"), with *King*, 569 U.S. at 445 ("The CODIS database is based on 13 loci at which the STR alleles are noted and compared.").

[142] See Presidential Comm'n for the Study of Bioethical Issues, Privacy and Progress in Whole Genome Sequencing, at app. IV (2012) [hereinafter Privacy and Progress], https://bioethicsarchive.georgetown.edu/pcsbi/sites/default/files/PrivacyProgress508_1.pdf [https://perma.cc/4F24-2NTF] (collecting state genetic laws, current to 2012).

Congress has also acted to preserve genetic privacy to a degree. In the Genetic Information Nondiscrimination Act of 2008 ("GINA"), Congress added "genetic information" to the scope of "health information" under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").[143] HIPAA, in turn, generally requires a covered entity to obtain authorization from an individual before disclosing her protected health information (including individually identifiable genetic information), unless a regulatory exception applies.[144] In addition, under the 21st Century Cures Act, federally-funded researchers receive a Certificate of Confidentiality, which requires those researchers to protect "identifiable, sensitive information" from disclosure.[145] Importantly, while the Act appears to permit disclosure of "identifiable, sensitive information" as "required by Federal, State, or local laws,"[146] this provision specifically excludes disclosures "in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding,"[147] unless those disclosures are "made with the consent of the individual to whom the information, document, or biospecimen pertains."[148]

To be sure, GINA, HIPAA, and the 21st Century Cures Act do not apply neatly to law enforcement use of consumer DNA platforms. For one thing, these platforms likely are not "covered entities" subject to HIPAA,[149] nor are the genetic analysis and genealogy services these platforms perform likely to constitute "research" under the 21st Century Cures Act in the ordinary course.[150] For another, unlike the seemingly-

[143] See 42 U.S.C. § 1320d-9(a)(1) (2012).

[144] 45 C.F.R. § 164.512 (2018) (setting forth regulatory exceptions to rule of required authorization).

[145] 42 U.S.C. § 241(d)(1)(A) (2012).

[146] Id. § 241(d)(1)(A), (d)(1)(C)(i).

[147] Id. § 241(d)(1)(D); see id. § 241(d)(1)(C)(i) (permitting disclosures "required by Federal, State, or local laws, *excluding instances described in subparagraph (D)*" (emphasis added)).

[148] Id. § 241(d)(1)(C)(iii); see id. § 241(d)(1)(D) (restricting disclosures "in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding . . . except in the circumstance described in subparagraph (C)(iii)").

[149] See, e.g., Natalie Ram, Christi J. Guerrini & Amy L. McGuire, Genealogy Databases and the Future of Criminal Investigation, 360 Sci. 1078, 1078 (2018) (explaining that HIPAA is unlikely to apply to consumer genetics services, as "[t]hese providers are usually careful to explain that they are not engaged in health care or the manipulation or provision of health data").

[150] See 42 U.S.C. § 241(d)(1)(A) (2012) (limiting Certificates to those engaged in "research," whether federally-funded (in which case a Certificate issues automatically) or not (in which case a Certificate may be issued "upon application by a person engaged in research")). Additional analysis and work conducted by consumer genetic services may, however,

strong protection against disclosure in the 21st Century Cures Act, HIPAA appears to permit covered entities to disclose genetic data for law enforcement use, so long as such disclosure is pursuant to some judicial process[151]—a far lesser requirement than the warrant the Fourth Amendment typically requires.[152]

But these misalignments need not undermine a general expectation of privacy in one's genetic data. GINA's stated purpose, to enable individuals to confidently "take advantage of genetic testing, technologies, research, and new therapies,"[153] evinces a general principle that genetic data is highly personal, sensitive, and worthy of protection from uninvited, prying eyes.[154] Moreover, as the Supreme Court has recently explained, the existence of an alternate compulsory process by which law enforcement may obtain otherwise private information is not inconsistent with an expectation of privacy in that information.[155]

Although the Court in *King* held that law enforcement may undertake a warrantless genetic search of a lawfully arrested individual,[156] it is unlikely that the Court would extend that reasoning to ordinary members of the public. *King* employed a balancing test, weighing "the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy."[157] In analyzing the "government[al] interest[s]" side of the ledger, the Court repeatedly emphasized

constitute research. For instance, 23andMe has obtained a Certificate of Confidentiality for its research-related work. See Research Consent Document, 23andMe, https://www.23andme.com/about/consent/ [https://perma.cc/E7JM-N83D] (last visited July 8, 2019) (explaining that "23andMe has obtained a Certificate of Confidentiality from the National Institutes of Health (NIH)" under "4. How do you keep my data protected and private (whether or not I consent)?").

[151] See 45 C.F.R. § 164.512(f) (2018).

[152] See Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) (observing that a court order under the Stored Communications Act "falls well short of the probable cause required for a warrant").

[153] Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, § 2(5), 122 Stat. 881, 882–83.

[154] See Bradley A. Arehart & Jessica L. Roberts, GINA, Big Data, and the Future of Employee Privacy, 128 Yale L.J. 710 (2019) (describing GINA's relative success as a privacy statute, at least in the workplace context, notwithstanding its failures as an anti-discrimination statute).

[155] See *Carpenter*, 138 S. Ct. at 2221 (holding that Stored Communications Act does not satisfy the Fourth Amendment with respect to historical cell site location information because "this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy").

[156] See 569 U.S. 435, 465 (2013).

[157] Id. at 448 (alteration in original) (internal quotation marks omitted).

that the interest at stake was "the need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody."[158] That is, "'[i]n every criminal case, it is known and must be known who has been arrested and who is being tried.'"[159] The Court explained that "[a] suspect's criminal history is a critical part of his identity that officers should know when processing him for detention," and that "[a] DNA profile is useful to the police because it gives them a form of identification to search the records already in their valid possession."[160] The Court also justified compulsory DNA sampling and CODIS searching as necessary for the safety of other detainees,[161] for assessing the appropriateness of bail,[162] and for facilitating exoneration of other wrongly convicted individuals.[163]

For the most part, these justifications for DNA profiling are inapplicable to ordinary members of the public, including those who take part in genealogical or other DNA testing. For one thing, it is not at all clear that the general balancing test the Court employed in *King* is an appropriate measure of Fourth Amendment interests when police seek to access genetic data to solve crimes. In general, the Court has required police to obtain a warrant before conducting a search, unless a recognized exception applies.[164] Indeed, although the Court in *King* insisted that its analysis was one of general "reasonableness," it nonetheless aligned its analysis with one such exception: the "special needs" cases.[165] Under the "special needs" doctrine, the government may obtain, analyze, and use information about an individual without a warrant or any prior suspicion of wrongdoing so long as the government's purpose is not for crime

[158] Id. at 449; see also id. at 461 ("In sum, there can be little reason to question 'the legitimate interest of the government in knowing for an absolute certainty the identity of the person arrested, in knowing whether he is wanted elsewhere, and in ensuring his identification in the event he flees prosecution.'" (quoting 3 W. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 5.3(c) (5th ed. 2012))).

[159] Id. at 450 (quoting Hiibel v. Sixth Judicial Dist. Court of Nev., 542 U.S. 177, 191 (2004) (alteration in original)).

[160] Id. at 450–51.

[161] Id. at 452.

[162] Id. at 453–55.

[163] Id. at 455–56.

[164] See supra note 53 and accompanying text; infra Part III (discussing whether privacy practices in consumer genetic services amount to consent to search, regardless of an expectation of privacy).

[165] See *King*, 569 U.S. at 463.

detection.[166] In *King*, the Court explained that King's DNA was being used to ascertain aspects of his "identity" that were relevant to arrest, detention, and other preliminary steps in a criminal proceeding.[167]

Conversely, individuals whose genetic data are stored in a genealogical or other database are in no sense in police "custody" or "detention." These individuals have not been arrested, nor are any of them specifically under suspicion in connection with a particular crime. Similarly, there is no sense in which comparing genetic data, including data stored in non-law enforcement databases, to DNA recovered from a crime scene is relevant to secure the "safety" of inmates in a local jail or for determining anything about bail, as none of the individuals from whom such genetic data is drawn are in detention or subject to bail. Rather, as to ordinary members of the public, police interests related to processing arrested or convicted individuals or securing the safety of officers or other inmates are simply inapposite.

On the "individual's privacy" side of the ledger, meanwhile, the Court observed that arrested individuals have diminished expectations of privacy by virtue of their arrest.[168] As the Court explained, the "special needs" cases need not justify DNA sampling because "unlike the search of a citizen who has not been suspected of a wrong, a detainee has a reduced expectation of privacy."[169] Once again, however, that reasoning is inapplicable to ordinary members of the public, including those whose genetic data is stored in a genealogical or other DNA database. These individuals are precisely "citizen[s] who ha[ve] not been suspected of a wrong."[170]

Thus, genetic data is data in which individuals can begin to claim a reasonable expectation of privacy.[171] That data is "deeply revealing."[172] It is also information that possesses sufficient depth and breadth to warrant

[166] See City of Indianapolis v. Edmond, 531 U.S. 32, 37, 41–42 (2000); Chandler v. Miller, 520 U.S. 305, 308 (1997); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989).

[167] See supra notes 158–163 and accompanying text.

[168] See *King*, 569 U.S. at 461–63; see also id. at 465–66 ("When officers make an arrest supported by probable cause to hold for a serious offense and they bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment.").

[169] Id. at 462–63.

[170] Id.

[171] See supra Section I.B.

[172] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); see also Ohm, supra note 92, at 384 (agreeing that genetic data satisfies *Carpenter*'s "deeply revealing nature factor").

constitutional scrutiny.[173] Properly sequenced genetic data can be highly detailed and precise about the individual information it discloses. Indeed, that is precisely why DNA has been lauded as the gold standard for forensic identification.[174] Moreover, a single cell contains the whole of an individual's genetic information, and that information can inform assessments about that individual's identity, genetic relatedness, physical traits, and even potential health risks.[175] The information even a single cell discloses may be both deep and broad in nature. Although the revealing nature of genetic data should not be mistaken for genetic exceptionalism,[176] the nature of that data makes it at least as sensitive as location data.

2. Sharing Genetic Data with a Service Provider Need Not Forfeit an Expectation of Privacy

The mere act of sharing genetic data with a third-party service provider ought not to automatically forfeit an expectation of privacy in genetic data. As set forth above, genetic data is "deeply revealing," and the information it discloses can be both deep and broad.[177] This data also satisfies, or soon will, each of the other factors the Supreme Court identified in its analysis in *Carpenter*, which focus on the ways in which data are collected and used by a third-party service provider.

Consider the comprehensives of the data at issue.[178] Although genetic analysis, whether by a direct-to-consumer firm or by another entity, may not yet be as widespread as cell phone usage, such analysis is growing rapidly. More than twenty-six million people have undertaken genealogical genetic analysis.[179] In 2017, the number of new users of consumer genetic services more than doubled the number of users in the previous

[173] *Carpenter*, 138 S. Ct. at 2223.

[174] See *King*, 569 U.S. at 442 ("[L]aw enforcement, the defense bar, and the courts have acknowledged DNA testing's unparalleled ability both to exonerate the wrongly convicted and to identify the guilty." (internal quotation marks omitted)).

[175] See supra notes 116–127 and accompanying text.

[176] See, e.g., James P. Evans & Wylie Burke, Genetic Exceptionalism: Too Much of a Good Thing?, 10 Genetics Med. 500 (2008); Mark Rothstein, Genetic Exceptionalism & Legislative Pragmatism, Hastings Ctr. Rep., July–Aug. 2005, at 27.

[177] See *Carpenter*, 138 S. Ct. at 2223 (identifying key factors for analysis); supra Subsection II.B.1.

[178] *Carpenter*, 138 S. Ct. at 2223 (relying on "comprehensive[ness]" to conclude that individuals have an expectation of privacy in their cell site location information).

[179] See Regalado, supra note 36.

year.[180] In 2018, "as many people purchased consumer DNA tests in 2018 as in all previous years combined."[181] According to one report, "[i]f the pace continues, the gene troves could hold data on the genetic makeup of more than 100 million people within 24 months."[182] Meanwhile, millions more have genetic data linked to their medical records, resulting from preconception, prenatal, cancer, or other medically related genetic analyses. In all, these widespread and growing uses suggest that genetic testing is a socially valuable activity that is an important part of many users' lives—and is one that is substantially growing its reach year over year. Today's direct-to-consumer marketplace may be akin to the early days of cell phone or smartphone use. After all, smartphone use exploded from only seventeen million handsets in April 2007[183] to more than 270 million active devices in 2017.[184]

Nor is use by even a plurality of Americans likely to be necessary for *Carpenter* to be satisfied. Scholars have already suggested in the wake of *Carpenter* that police access to data collected by smart home devices, including Amazon Echos, Smart TVs, or Nest thermostats, are likely to require a warrant.[185] Yet these devices, like consumer genetic services, are similarly not-quite-ubiquitous.[186]

Like cell site location information, genetic data also enables the government to conduct its investigations in "remarkably easy, cheap, and efficient [ways,] compared to traditional investigative tools," such as "[w]ith just the click of a button."[187] Once sequenced, it is nearly costless to search genetic data for similar profiles, even where the individual to be

[180] See Antonio Regalado, 2017 Was the Year Consumer DNA Testing Blew Up, MIT Tech. Rev. (Feb. 12, 2018), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up/ [https://perma.cc/D7JN-JQ66].

[181] Regalado, supra note 36.

[182] Id.

[183] See Charles Arthur, The History of Smartphones: Timeline, Guardian (Jan. 24, 2012), https://www.theguardian.com/technology/2012/jan/24/smartphones-timeline [https://perma.cc/HXK7-VP8J].

[184] See Smartphones in Active Use, Cellular Telecomms. Indus. Ass'n, https://www.ctia.org/the-wireless-industry/infographics-library [https://perma.cc/RN2R-NKZ5].

[185] See, e.g., Kaminski, supra note 63; Ohm, supra note 92, at 394–96.

[186] See, e.g., NPR & Edison Research, The Smart Audio Report 2 (2019) (reporting that "21% of people in the U.S. 18+ own a Smart Speaker, or around 53 million people"); Jeff Baumgartner, Study: 74% of U.S. TV Homes Have at Least One Connected TV Device, Multichannel News (June 8, 2018), https://www.multichannel.com/blog/study-74-u-s-tv-homes-have-at-least-one-connected-tv-device [https://perma.cc/8GZS-NDA2] (reporting that, in 2018, "about 29% of all TVs in U.S. homes are connected smart TVs").

[187] Carpenter v. United States, 138 S. Ct. 2206, 2218 (2018).

matched is unknown. Indeed, this is precisely what genealogical genetic platforms do, sometimes for no charge at all.[188] In this respect, genetic genealogy databases might be viewed as super-charged versions of the CODIS database.

Finally, genetic data aggregated in genealogical databases may be approaching an "inescapable and automatic nature" that makes the sharing of such data not truly "voluntary."[189] To be sure, individuals currently undertake consumer genetic testing largely voluntarily and intentionally. The *Carpenter* Court observed, however, that Fourth Amendment analysis of expectations of privacy should take account not only of technology currently in use, but also "of more sophisticated systems that are already in use or in development."[190] As set forth above, the use of consumer genetic testing services is growing rapidly, with gains of more than 100% year over year.[191] Over time, failure to have obtained genetic analysis, whether through a direct-to-consumer firm or other entity, may well become as unusual and exceptional as one's failure to carry a cellular device.

Moreover, even today, there are aspects of automaticity and involuntariness in genetic analysis. For one thing, once sequenced and stored, genealogical genetic platforms return new results automatically and passively, without further input from the user.[192] For another, the nature of genetic data as a unique identifier really is "inescapable and automatic." That is precisely why CODIS comparison has become a gold standard for forensic identification and crime solving.[193]

In sum, courts should recognize that individuals have an expectation of privacy in their genetic data, and the mere sharing of that data with a third party ought not negate that expectation. These expectations of privacy are

[188] See, e.g., GEDmatch, https://www.gedmatch.com/login1.php [https://perma.cc/BR83-RU2P] (last visited July 17, 2019) ("GEDmatch provides applications for comparing your DNA test results with other people. There are also applications for estimating your ancestry. Some applications are free. More advanced applications require membership in the GEDmatch Tier1 program at $10 per month.").

[189] *Carpenter*, 138 S. Ct. at 2220, 2223.

[190] Id. at 2210 (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

[191] See supra notes 179–182 and accompanying text.

[192] See, e.g., Preferences: Notifications, Consent, Report Configuration, 23andMe, https://-customercare.23andme.com/hc/en-us/articles/202907570-Preferences-Notifications-Consent-Report-Configuration [https://perma.cc/CW3W-AULR] (last visited Aug. 15, 2019) (identifying "new DNA Relatives" among available email notifications).

[193] See Maryland v. King, 569 U.S. 435, 442 (2013) ("[L]aw enforcement, the defense bar, and the courts have acknowledged DNA testing's unparalleled ability both to exonerate the wrongly convicted and to identify the guilty." (internal quotation marks omitted)).

distinct from, and weightier than, those the Supreme Court considered in *King*, and so warrantless access despite an expectation of privacy is unlikely to prevail, absent alternative justification.

Indeed, in some ways, users of consumer genetic services have stronger claims to expectations of privacy in genetic data about them than cell phone users have in their location data. Each of the dissenting Justices in *Carpenter* suggested that a property interest in the records to be disclosed should be an essential component of the Fourth Amendment inquiry.[194] For several of these Justices, their conclusion that Carpenter did not have a property interest in the records to be disclosed was dispositive.[195] By contrast, the terms of use for consumer genetic services routinely and unequivocally acknowledge that users have a property interest in their individual-level genetic data. Ancestry's terms and conditions are particularly blunt: "You always maintain ownership of your data . . . ."[196] 23andMe's terms of service, while more longwinded, amount to largely the same thing: "Any Genetic Information derived from your saliva remains your information, subject to rights we retain as set forth in these [terms of service]."[197] Even GEDmatch, which promises little in the way of privacy,

[194] See *Carpenter*, 138 S. Ct. at 2235–36 (Thomas, J., dissenting) ("The Court concludes that, although the records are not Carpenter's, the Government must get a warrant because Carpenter had a reasonable 'expectation of privacy' in the location information that they reveal. I agree with Justice Kennedy, Justice Alito, Justice Gorsuch, and every Court of Appeals to consider the question that this is not the best reading of our precedents." (citation omitted)).

[195] See id. at 2226 (Kennedy, J., dissenting) ("Here the only question necessary to decide is whether the Government searched anything of Carpenter's when it used compulsory process to obtain cell-site records from Carpenter's cell phone service providers. This Court's decisions in *Miller* and *Smith* dictate that the answer is no . . . ."); id. at 2235 (Thomas, J., dissenting); id. at 2247 (Alito, J., dissenting) (criticizing the Court for "allow[ing] a defendant to object to the search of a third party's property" and describing this as "revolutionary"). But see id. at 2272 (Gorsuch, J., dissenting) (agreeing with dissenters that property concepts are essential to the Fourth Amendment inquiry but suggesting that it is "entirely possible a person's cell-site data could qualify as *his* papers or effects under existing law").

[196] Ancestry Terms and Conditions, Ancestry (June 5, 2018), https://www.ancestry.com/cs/legal/termsandconditions [https://perma.cc/HTU8-4Z9L]; see also Ancestry Privacy Philosophy, Ancestry, https://www.ancestry.com/cs/privacyphilosophy [https://perma.cc/VD9N-FYGK] (last visited July 17, 2019) (under "Your Data," in response to the question, "Who owns my data?," stating, "You own your DNA data and you can ask us to remove your data from our systems at any time. We do not keep copies unless you have consented to participate in research, in which case only those research projects that are ongoing or completed will contain your data.").

[197] Terms of Service, 23andMe [hereinafter 23andMe Terms of Service], https://www.23andme.com/about/tos/ [https://perma.cc/C83Y-ZTWY] (last visited July 17, 2019).

nonetheless recognizes that its users own the data they upload.[198] Insofar as the Fourth Amendment inquiry may turn on the strength of the property interest involved, users of genealogical genetic services are in a much better position to assert an expectation of privacy in their data than are cell phone users.

III. REBUILDING PRIVACY PRACTICES AFTER *CARPENTER*

The role of third-party intermediaries in shaping Fourth Amendment expectations of privacy has been a subject of judicial and academic debate for many years. That debate has intensified as more of daily life has become digital and dependent on such intermediaries, and as more technology has become a staple of modern living. Yet, little scholarly attention has focused on the role of third-party privacy practices in shaping the Fourth Amendment privacy protections.[199] In one sense, this is unsurprising. Under pre-*Carpenter* doctrine, merely disclosing that a service provider "collect[s]"[200] or "retain[s]"[201] user data was generally sufficient to render the Fourth Amendment inapplicable to police conduct.

Section III.A first delineates the limited and limiting role of privacy practices under pre-*Carpenter* doctrine. Section III.B considers whether there is any legitimate role for these practices after *Carpenter*, concluding that, in appropriate circumstances, they may inform a more robust assessment of consent to search, notwithstanding a reasonable expectation of privacy.

A. A Limited Role for Third-Party Privacy Practices

Until *Carpenter*, privacy practices of third-party intermediaries largely played a singular role in Fourth Amendment cases—as indicia that there was no Fourth Amendment protection for activities conducted in digital

[198] See GEDmatch.com Terms of Service and Privacy Policy, supra note 20 ("Raw DNA data uploaded to GEDmatch.Com ('Raw Data') remains the property of the person who uploaded it.").

[199] But see Tokson, supra note 54, at 174–75 (criticizing the role of privacy policies in Fourth Amendment analysis as an inaccurate measure of user knowledge); Eric Johnson, Note, Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data, 69 Stan. L. Rev. 867, 898–900 (2017) (arguing that terms of service policies may affect the expectations of privacy that users of cloud storage services have in their remotely stored data).

[200] In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013).

[201] In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 136 (E.D. Va. 2011).

media.[202] Courts frequently seized upon the privacy policies and terms of service of network platforms almost exclusively to undermine expectations of privacy.[203] Indeed, in nearly every case, so long as a policy disclosed the collection, retention, or use of an individual's data, that user was charged with knowledge of that disclosure and with a commensurate lack of expectation that their data might remain private at all.[204]

Supreme Court doctrine governing expectations of privacy in data shared with a third party largely dictated that result. Lower courts, applying the strong pre-*Carpenter* third-party principle to emerging digital technologies, often turned to privacy policies and terms of use to discern whether users had "voluntarily conveyed"[205] or "knowingly expose[d]"[206] their data to third-party collection. In many instances, courts construed these policies broadly to undermine any expectation of privacy in user data. Thus, the U.S. Court of Appeals for the Fifth Circuit concluded that a cell phone user could not maintain an expectation of privacy in his historical cell site location information where "contractual terms of service and providers' privacy policies expressly state that a provider uses a subscriber's location information to route his cell phone calls" and "inform subscribers that the providers not only use the information, but collect

[202] See, e.g., *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d at 613; United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) ("We conclude that the remote searches of Simons' computer did not violate his Fourth Amendment rights because, in light of the Internet policy, Simons lacked a legitimate expectation of privacy in the files downloaded from the Internet."); *In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d at 136 (finding that there was no expectation of privacy in users' IP address information in part because "[n]o party disputes that the Privacy Policy permits Twitter to retain Petitioners' IP address information"); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005) (finding no expectation of privacy in ISP subscriber information, despite "an agreement between the defendant and AOL that limited AOL's right to release his biographical data to third parties" because that agreement permitted disclosures to the government "in response to legal process, such as a court order or subpoena, or in special cases such as a physical threat to you or others"); see also Tokson, supra note 54, at 174–75 (collecting cases). But see United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) (relying in part on privacy policy silence on the matter of ISP access to email content in holding that individuals retain an expectation of privacy in such content); United States v. Heckenkamp, 482 F.3d 1142, 1146–47 (9th Cir. 2007) (observing that a university's computer policy reinforces a user's expectation of privacy in his computer, but holding that a search of Heckenkamp's computer was nonetheless justified by a "special need[]").

[203] See Johnson, supra note 199, at 898–99 ("Many courts have held that terms of service affect a user's reasonable expectation of privacy by defining the amount of privacy the user relinquishes." (footnote omitted)).

[204] See supra note 202.

[205] Smith v. Maryland, 442 U.S. 735, 744–45 (1979).

[206] United States v. Miller, 425 U.S. 435, 442 (1976).

it."[207] Another court found that disclosure in a privacy policy that a third-party service provider would "retain" a user's IP address information vitiated an expectation of privacy in that data.[208] And another held that even where a privacy policy purported to limit a digital service provider's ability to disclose a user's "biographical data" to others, no expectation of privacy would attach so long as that contract also included boilerplate language permitting disclosure "in response to legal process, such as a court order or subpoena."[209]

More rarely, courts interpreted privacy policies to protect user privacy against government intrusion. Even in these instances, however, courts concluded that privacy prevailed because of what a privacy policy did *not* say, rather than because of what it did say. In *United States v. Warshak*, for instance, the Sixth Circuit concluded that a user retained an expectation of privacy in the content on his email communications, even though the user's internet service provider had "control" over the emails and "ability to access them under certain limited circumstances."[210] *Warshak* emphasized that the subscriber agreement nonetheless left the user with an expectation of privacy because it did not disclose the ISP's intention to "audit, inspect, and monitor" its subscribers' communications.[211] The court explained that it was "unwilling to hold that a subscriber agreement will *never* be broad enough to snuff out a reasonable expectation of privacy."[212] But the court did not appear to entertain the possibility that affirmative language in the privacy policy could protect the user, rather than undermine her privacy. *Warshak*'s reasoning may also have deferred less to third-party doctrine concerns than many other cases because of the particular data it involved: the content of email communications. In such cases, courts have more frequently analogized to letters placed in the hands of mail carriers than to bank records or phone numbers.[213]

---

[207] *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d at 613.

[208] In re Application of U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 136 (E.D. Va. 2011).

[209] United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005) (internal quotation marks omitted).

[210] 631 F.3d 266, 287 (6th Cir. 2010).

[211] Id. (internal quotation marks omitted) (quoting Warshak v. United States, 490 F.3d 455, 472–73 (6th Cir. 2007)).

[212] Id.

[213] See id. at 285–86 ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) ("E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its

Moreover, at least one court concluded that the terms of use and privacy policy of a service provider affirmatively bolstered, rather than undermined, a user's expectation of privacy. In *United States v. Heckenkamp*, the Ninth Circuit concluded that a computer user did not forfeit his expectation of privacy in his computer and its files merely by connecting it to a public university network.[214] The court explained that, in the absence of an "announced monitoring policy on the network," "the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer."[215] Significantly, the court cited affirmative privacy commitments in the university's computer policy as reinforcing, rather than undermining, an expectation of privacy. "When examined in their entirety, university policies do not eliminate Heckenkamp's expectation of privacy in his computer. Rather, they establish limited instances in which university administrators may access his computer in order to protect the university's systems."[216]

Unfortunately, *Heckenkamp* was largely an outlier. Other courts faced with policies similarly establishing limited grounds for provider disclosure of user information nonetheless concluded that no expectation of privacy could attach, as even limited grounds were deemed to negate such expectations.[217]

In sum, courts in the pre-*Carpenter* era were not shy about considering the language of third-party privacy policies, terms of use, and related documents in assessing Fourth Amendment expectations of privacy. The resulting analysis, however, was quite limited and almost singularly one-sided, with a variety of typical disclosures resulting in a total forfeiture of users' Fourth Amendment privacy interests. As discussed in Section III.B, *Carpenter* may open the way to reframe the role of third-party privacy

intended location, and also a package of content that the sender presumes will be read only by the intended recipient. The privacy interests in these two forms of communication are identical. The contents may deserve Fourth Amendment protection, but the address and size of the package do not."); see also Carpenter v. United States, 138 S. Ct. 2206, 2230 (2018) (Kennedy, J., dissenting) (conceding that "*Miller* and *Smith* may not apply when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party" and citing *Warshak* approvingly).

[214] 482 F.3d 1142, 1146–47 (9th Cir. 2007).

[215] Id.

[216] Id. at 1147.

[217] See, e.g., United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005).

practices as indicia of consent to search, yielding a more robust and nuanced analysis of practices writ large.

B. Rebuilding Privacy Practices as Consent

Carpenter had little to say directly about third-party privacy practices. To be sure, in considering how private cell site location information is, the Court noted both legal constraints on how this information is used, as well as less formal constraints like the collection and sales practices of cell phone service providers. The Court observed that "[w]ireless carriers collect and store [cell site location information] for their own business purposes, including finding weak spots in their network and applying 'roaming' charges when another carrier routes data through their cell sites."[218] The Court further acknowledged that "wireless carriers often sell aggregated location records to data brokers," but "without individual identifying information of the sort at issue here."[219]

Although these observations might have reflected uses of user information permitted by, and disclosed in, user terms of service and privacy policies, the Court's opinion did not cite those policies.[220] Nor did the Court's descriptions associate these privacy-related practices with a specific cell phone user agreement, using instead general terms to describe what "wireless carriers" do, rather than what Sprint and MetroPCS do. Thus, it may be fair to say that, after *Carpenter*, third-party privacy practices play an equal, but opposite, role to the one they played before the *Carpenter* decision. That is, after *Carpenter*, third-party privacy practices may play little or no role in determining whether certain data may be the subject of a reasonable expectation of privacy.

This does not mean, however, that privacy practices are wholly immaterial to Fourth Amendment analysis writ large. After all, Fourth Amendment analysis does not end with the conclusion that an expectation of privacy is reasonable. Rather, Fourth Amendment doctrine is riddled with exceptions to the requirement that police obtain a warrant before breaching a reasonable expectation of privacy. Among these is the doctrine of consent, which holds that a search conducted with the consent of one authorized to give it is reasonable, and thus may be conducted even absent

[218] *Carpenter*, 138 S. Ct. at 2212.
[219] Id.
[220] Id.

probable cause or a warrant.[221] That third-party privacy practices might operate as consent to search is not without precedent. Indeed, Professor Orin Kerr has previously argued that the third-party doctrine itself is best understood as a consent doctrine.[222] Others have similarly acknowledged the important role of third-party privacy practices as indicia of user consent and understanding.[223]

After *Carpenter*, it would go too far to remake the third-party doctrine in the guise of consent. Indeed, *Carpenter*'s refusal to explicitly consider cellular providers' privacy practices in resolving the case stands as a sharp rebuke to a too-lax acceptance of user agreements as consent. But the choices of private entities about whether and how to collect, store, and share user information—and communicate with users about those choices—will necessarily inflect Fourth Amendment analysis going forward.[224] As Professor Paul Ohm has observed, after *Carpenter*, "[n]ot only does the mere fact that a target trusted personal information with a third party no longer insulate that data from Fourth Amendment scrutiny, but also the Constitutional duties imposed on the police might now turn on the independent decisions of third parties."[225]

Thus, privacy policies and practices may, in appropriate circumstances, serve as a valid source of consent to search by the government. Privacy practices do much more than inform users about the internal collection and use of user data. Such policies and practices shape whether, how, and in what ways user data is made available to other third parties. Privacy policies and related practices can disclose whether a digital service provider adheres to industry best standards for user privacy and data protection, promises to inform users about government requests for their data,

[221] See Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

[222] See Orin Kerr, The Case for the Third-Party Doctrine, 107 Mich. L. Rev. 561, 587–90 (2009) (arguing that the third-party doctrine is best understood as a consent doctrine).

[223] See Hernandez, supra note 29 (quoting Debbie Kennett, "a British genealogy enthusiast and honorary research associate at University College London," as saying "I don't think it's right for law enforcement to use a database without the informed consent of the consumer"); Kristen Carosa, Investigators Turn to Genealogy Databases to Solve Old Crimes, WMUR, (Nov. 12, 2018, 10:00 PM), https://www.wmur.com/article/investigators-turn-to-genealogy-databases-to-solve-old-crimes/25018859 [https://perma.cc/CDU8-JPDV] (quoting Albert Scherr, Professor of Law, University of New Hampshire School of Law, explaining, "The database is taking this information from these people without informing them they may use it for this purpose. . . . If they said, 'By the way, by contributing your profile at X amounts of genetic locations, you are authorizing us (to release information) if the police ask,' then that it is fine").

[224] See Ohm, supra note 92, at 390–92.

[225] Id. at 392.

or sells its users' data to third parties who may voluntarily assist the government in surveillance efforts.[226]

To be sure, there is a robust literature identifying and criticizing overreliance on "consent" as a tool for effective digital consumer governance.[227] Consent may be a fiction where disclosure of important privacy practices "is buried somewhere in a dense privacy policy."[228] Empirical evidence demonstrates that few users read these types of documents in whole or even in part.[229] In one study of online purchasers' engagement with end-user license agreements (that is, terms of use), researchers found that only a fraction of one percent of purchasers examine a product's license agreement for even one second.[230] Such a small likelihood of active engagement cannot reasonably be said to sufficiently inform a user about the service provider's approach to user privacy to give rise to genuine consent. Moreover, failure to access terms of service and similar online documents may be entirely rational. These documents are often long, vague, and written in far too abstruse language for the average American reader. According to one estimate, end-user license agreements average nearly 2,000 words each and require a college degree to understand their language fully.[231]

Professors Neil Richards and Woodrow Hartzog have supplied a taxonomy for identifying the "pathologies of digital consent"—ways in which digital consent may derogate from the knowing and voluntary "gold standard" to which the law typically adheres.[232] In their taxonomy,

[226] See Nate Cardozo et al., Who Has Your Back?, Elec. Frontier Found. 11–16 (2017), https://www.eff.org/files/2017/07/08/whohasyourback_2017.pdf [https://perma.cc/L3B9-N-ND7].

[227] See, e.g., Neil Richards & Woodrow Hartzog, The Pathologies of Digital Consent, 96 Wash. U. L. Rev. (forthcoming 2019) (manuscript at 2 & n.3) (on file with Virginia Law Review Association) (observing that "a number of privacy law scholars (including ourselves) have documented, while consent models permeate the digital consumer landscape, the practical conditions of these agreements fall far short of the gold standard," and collecting sources).

[228] Id. at 3.

[229] See Yannis Bakos et al., Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts, 43 J. Legal Stud. 1 (2014).

[230] Id. at 3 (reporting that only 0.2% of purchasers access the end-user license agreement for one second or longer).

[231] See Florencia Marotta-Wurgler & Robert Taylor, Set in Stone? Change and Innovation in Consumer Standard-Form Contracts, 88 N.Y.U. L. Rev. 240, 253 (2013).

[232] See Richards & Hartzog, supra note 227. In Fourth Amendment doctrine, consent ought likewise be knowing and voluntary in order to be constitutionally valid, see Georgia v. Randolph, 547 U.S. 103, 109 (2006) (describing the "voluntary consent" exception to the warrant requirement); Bumper v. North Carolina, 391 U.S. 543, 548 (1968) (explaining that consent

consent is invalid where it is "unwitting," "coerced," or "incapacitated."[233] That is, Richards and Hartzog challenge the application of the term "consent" to practices that undermine either the "knowing" or "voluntary" attributes of consent itself.

Nonetheless, as Richards and Hartzog acknowledge, consent is—and must remain—an important and valuable legal tool.[234] Thus, courts should take *Carpenter* as an opportunity to deepen their consideration of service providers' substantive privacy commitments through the rubric of consent. Privacy practices, which frequently memorialize provider approaches to user privacy more broadly, may guide judicial consideration of whether an individual has validly waived her expectation of privacy in data about her. Indeed, because a service provider's mere access to or use of user data does not negate a user's expectation of privacy in their sensitive data, statements and policies about a service provider's efforts to protect user privacy more broadly—particularly vis-a-vis the government itself—may reinforce an expectation of privacy in shared data. Concomitantly, where a service provider explicitly informs its users that it will share their individual-level data with others, and particularly with the government—and particularly if the service requires users actively to choose such sharing—agreement may amount to consent. Such users should hardly be surprised when the service provider does, in fact, cooperate with police.

The scope of what that consent requires in the third-party context, however, must necessarily be more narrowly drawn and more substantive in nature after *Carpenter*. Disclosures must be robust to constitute a valid waiver of an expectation of privacy in sensitive personal data. And if disclosures are to be more robustly examined, then the Fourth Amendment may properly draw a "distinction between third parties that want to shield [your] confidence and those that do not."[235]

Taking Richards and Hartzog's "pathologies of digital consent" as a helpful taxonomy, this Section identifies guideposts that may inform judicial determinations about whether an individual's agreement to and

must be "freely and voluntarily given"); although those requirements may be assessed under a totality of the circumstances, see Schneckloth v. Bustamonte, 412 U.S. 218, 226–27 (1973), or "inferred from context," Birchfield v. North Dakota, 136 S. Ct. 2160, 2185 (2016).

[233] Richards & Hartzog, supra note 227, at 5–6, 18–36.

[234] Id. at 4.

[235] Erin Murphy, The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr, 24 Berkeley Tech. L.J. 1239, 1252 (2009).

interaction with a service provider's privacy practices amounts to valid consent to police search.[236] Of course, whether such agreement amounts to valid consent will, inevitably, be a matter of degree. That assessment will turn substantially on what is disclosed—and how.

First, in order for consent to be valid, the user must have had a genuine opportunity for decision making. The absence of such opportunity is precisely the problem of "coerced consent" in Richards and Hartzog's taxonomy—"a choice that takes the 'voluntary' out of 'knowing and voluntary.'"[237] As the Seventh Circuit recently recognized in a decision applying *Carpenter* to find a reasonable expectation of privacy in data from a smart meter, "a choice to share data imposed by fiat is no choice at all."[238] In *Naperville Smart Meter Awareness v. City of Naperville*, the court explained, the only provider of municipal electricity also required participation in a smart meter program.[239] A choice between electric service and no electric service in the home was not a genuine choice the law would recognize. Similarly, in *Carpenter*, the ubiquity and modern role of the cell phone—and the similar privacy practices across the industry—undermined any sense of consent to use such a phone or the location tracking that accompanies it.[240] Thus, in the absence of genuine options, no consent is possible.

Second, even where a marketplace offers multiple and genuine alternatives, mere boilerplate language that a service provider will disclose user data "as required by law" should not suffice to waive a user's expectation of privacy in otherwise sensitive and private data. Under Richards and Hartzog's taxonomy, such boilerplate language—typically buried in a long and dense privacy policy—risks "unwitting consent," or the high likelihood that "most consumers don't know what data practices are possible, what they have agreed to, or what the informational risks of the transaction are."[241] Such consent is problematic because it "takes the 'knowing' out of 'knowing and voluntary.'"[242]

[236] See also infra Part IV (considering the specific privacy policies of genealogical DNA databases in light of *Carpenter*, which may help give further content to this standard).

[237] Richards & Hartzog, supra note 227, at 28–29 (emphasis omitted).

[238] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018).

[239] Id. at 524.

[240] See Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[241] Richards & Hartzog, supra note 227, at 19.

[242] Id.

Like a requirement of a genuine opportunity for user choice, a more-than-boilerplate requirement is also evident in *Carpenter* itself. As is typical in privacy policies and terms of service, Sprint's privacy policy states that Sprint "may access, monitor, use or disclose your personal information or communications to . . . comply with the law or respond to lawful requests or legal process."[243] MetroPCS's privacy policy similarly discloses, "[w]e may disclose Personal Information, and other information about you, or your communications, where we have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary . . . to satisfy any applicable law, regulation, legal process or enforceable governmental request."[244] These are standard disclosure terms, and were likely already in place at the time Carpenter possessed and used the cell phone at issue in *Carpenter*. Yet, the Court nonetheless held that Carpenter retained a valid Fourth Amendment expectation of privacy in the cell phone location data that Sprint and MetroPCS collected.[245]

Third, to further avoid "unwitting consent," explicit language that goes beyond boilerplate and that is specific to government access should be particularly informative to assessments of Fourth Amendment consent to search. To be sure, where data is truly public and open to all, a specific invitation to the government may not be required to conclude that an individual has waived her expectation of privacy in otherwise sensitive data.[246] But where data is shared in a more limited fashion, policy-based

[243] Sprint Corporation Privacy Policy, Sprint (May 2, 2014), https://wholesale.sprint.com/-your-privacy-rights [https://perma.cc/6S85-24ZH] (describing "Information We Share" for the "Protection of Sprint and Others").

[244] Metro by T-Mobile Privacy Policy, MetroPCS (Mar. 22, 2019), https://www.metropcs.com/content/metro/en/desktop/metro/terms-conditions/privacy.html [https://perma.cc/BW2D-74F4] (describing "When We Share Information Collected About You: For Legal Process & Protection").

[245] See *Carpenter*, 138 S. Ct. at 2217.

[246] See, e.g., United States v. DiTomasso, 56 F. Supp. 3d 584, 592 (S.D.N.Y. 2014) (acknowledging that a forum "'open to all who cared to enter' . . . clearly falls beyond the scope of Fourth Amendment protection," but declining to find that the particular platform at issue was in fact '"open to all'" (quoting Government's Opposition to Defendant's Motion to Suppress at 11, *DiTomasso*, 56 F. Supp. 3d 584)); Steven D. Zansberg & Janna K. Fischer, Privacy Expectations in Online Social Media–An Emerging Generational Divide?, 28 Comm. Law., Nov. 2011, at 1, 27 (observing that, in the context of civil discovery, several courts have concluded that "information that is available to all on the Internet," such as a public MySpace page, "is not entitled to a reasonable expectation of privacy," "even if it was subjectively intended only to be seen by a limited audience"); id. (observing that emerging doctrine in the civil context suggests that "courts will view information posted on a publicly available social

restrictions on government access may inform a user about the extent of her privacy. Indeed, Justice Gorsuch acknowledged as much in a friendly dissent in *Carpenter*.[247] "Consenting to give a third party access to private papers that remain my property," Justice Gorsuch explained, "is not the same thing as consenting to a *search of those papers by the government*."[248] Consistent with this insight, where an individual has unmistakably agreed to "a search . . . by the government," it is appropriate to treat that consent as valid.[249] Conversely, when an intermediary has affirmatively and explicitly denounced government cooperation (or has declined explicitly to disclose such an approach), an expectation of privacy ought properly to gain even greater force through reinforcement.

Fourth, privacy practices should carry more weight in judicial assessments of user consent the more explicit, visible, and understandable they are—that is, the more they approach a model of genuine knowing and voluntary consent, and avoid the pathologies of unwitting, coerced, and incapacitated consent. Terms of service, privacy policies, and other online documents may go some ways to disclosing to users a service provider's approach to user privacy, including vis-a-vis the government. But it is not at all clear that these documents, standing alone, can sufficiently disclose reasonable risks to a user to amount to a valid waiver of an otherwise reasonable expectation of privacy. After all, imputing detailed knowledge of digital service providers' terms of service and privacy policy

media site as not entitled to any privacy protection (regardless of how few people actually accessed the information) and may well treat as private information whose access is restricted to a class of people (not open to all) even if it is a large class").

[247] Justice Gorsuch dissented on the grounds that Carpenter had not briefed or presented an argument that he should prevail based on property or possessory rights secured to him under positive law. *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting). Nonetheless, Justice Gorsuch's opinion quite clearly indicated that the Justice is receptive to curtailing warrantless government access to personal data shared with another. See id. at 2262 ("Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of *Katz*. But that result strikes most lawyers and judges today—me included—as pretty unlikely.").

[248] Id. at 2263.

[249] Cf. *DiTomasso*, 56 F. Supp. 3d at 597 (concluding that the defendant consented to a search of his emails for law enforcement purposes when he agreed to a terms of use policy that "makes clear that AOL intends to actively assist law enforcement," while declining to find such consent where a policy "includes only a passing reference to law enforcement—and which gives no indication of the role [the service provider] intends to play in criminal investigations").

documents may tax credulity.[250] As described above, empirical data indicate that few users read these documents even in part[251]—and that such avoidance may be entirely rational.[252]

But not all privacy practices are equally uninformative to the reasonable user. Service providers can encourage their users to engage with terms of service, privacy policies, and similar documents by requiring more direct interaction with these documents during the process of signing up for or using a service. Thus, over time, license agreements have shifted from largely pay-now-terms-later[253] agreements to a greater proportion of browsewrap[254] and clickwrap agreements.[255] (None of these modes of disclosure have, to date, yielded a high rate of readership, perhaps in part because more easily accessible policy documents are also, on average, longer and even more difficult to read than their less-accessible counterparts.)[256]

Moreover, principal privacy terms need not be hopelessly buried in too-long and highly technical documents. Online service providers may consolidate key terms in plain language at the top of a policy document so that users can more easily gain a basic understanding of the policy's terms.[257] Some online service providers have also begun to summarize key privacy practices on their homepages, in easy-to-find and easy-to-understand ways.[258] In other instances, other third parties have done the work of reading, analyzing, and digesting privacy policies and related documents and making their basic terms more easily accessible and comparable. The Electronic Frontier Foundation, for instance, has published

[250] See Tokson, supra note 54, at 174–75 (describing empirical findings that most users do not understand the purpose of, let alone read, terms of service and privacy policy documents, in part, because reading such documents would be prohibitively laborious).

[251] See Bakos et al., supra note 229, at 19–22.

[252] See Marotta-Wurgler & Taylor, supra note 231, at 253.

[253] In which consumers can access their terms of use only after purchasing the product in question. See Florencia Marotta-Wurgler, Even More than You Wanted to Know About the Failures of Disclosure, 11 Jerusalem Rev. Legal Stud. 63, 66 (2015).

[254] In which contracts "are posted on the seller's web site but require individuals to click on a hyperlink that may or may not be easy to find." Id.

[255] In which consumers must click on "I agree" to complete a purchase. Id.

[256] Id. at 68.

[257] See, e.g., Privacy Highlights, 23andMe (July 17, 2018) [hereinafter 23andMe Privacy Highlights], https://www.23andme.com/about/privacy/ [https://perma.cc/M5MA-RJM6] (disclosing "an overview of some core components of our data handling practices" before setting out the "Full Privacy Statement").

[258] See infra notes 280–290 and accompanying text (describing summaries of privacy practices on 23andMe and Ancestry websites).

annual reports that "turn a spotlight on how the policies of technology companies either advance or hinder the privacy rights of users when the U.S. government comes knocking."[259] And while "privacy markets . . . have largely failed to function" effectively in many ways,[260] there is a recent trend of digital service providers embracing user privacy—at least vis-a-vis the government and in at least some circumstances.[261]

Locating privacy practices in the Fourth Amendment doctrine of consent, moreover, correctly mandates that courts consider whether a reasonable, or even a particular, user would have been aware of and understood a service provider's privacy practices. The more explicit, visible, and understandable those practices are, the greater weight they should receive in the Fourth Amendment inquiry.

Indeed, robust analysis of service providers' privacy policies and related practices in the Fourth Amendment context might help drive more demanding judicial analysis of privacy practices more broadly. Courts have often deferred to terms of use and privacy policies as enforceable disclaimers, even where those policies are unreadable or difficult for ordinary users to understand or find.[262] But a judicial norm in the Fourth Amendment setting that enforces a limited set of privacy disclaimers—those that are sufficiently explicit, visible, and understandable to

[259] Cardozo et al., supra note 226, at 4.

[260] Tokson, supra note 54, at 168; see also Julie E. Cohen, Irrational Privacy?, 10 J. Telecomm. & High Tech. L. 241, 242 (2012) (arguing that scholars have recognized that privacy markets are prone to significant market failure).

[261] Cardozo et al., supra note 226, at 7 ("Every company we evaluate has adopted baseline industry best practices, such as publishing a transparency report and requiring a warrant before releasing user content to the government."); Future of Privacy Forum, Privacy Best Practices for Consumer Genetic Testing Services 7–9 (2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf [https://perma.cc/F3UZ-9XYZ]. Interestingly, competition on differing privacy terms may be a salient feature of consumer genetics platforms in particular. As discussed in Part IV, infra, 23andMe and Ancestry have made strong public statements about their commitment to shielding user genetic data from law enforcement access. Meanwhile, FamilyTreeDNA has advertised exactly the opposite, inviting potential users to join its service precisely because of its relationship with law enforcement.

[262] See, e.g., Mark A. Lemley, Terms of Use, 91 Minn. L. Rev. 459, 459 (2006) ("[M]ore and more courts and commentators seem willing to accept the idea that if a business writes a document and calls it a contract, courts will enforce it as a contract even if no one agrees to it."); id. at 467 (describing the growing judicial acceptance of "shrinkwrap" licenses, which are "license[s] packaged within the shrinkwrap or loaded on the computer and provide[] that breaking the shrinkwrap or running the program constitute[s] acceptance of the terms of the contract"); Richards & Hartzog, supra note 227, at 3; see also ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996) (enforcing shrinkwrap license).

genuinely inform a reasonable person's understanding about their privacy—may encourage a similarly more demanding standard for privacy waivers even for non-law enforcement practices.[263]

Finally, reliance on privacy policies and practices in the Fourth Amendment setting need not negate efforts to urge service providers to adhere to more protective policies overall—or to require them to do so through recognition of common law fiduciary-like duties.[264] Nor should judicial consideration of third-party privacy practices undermine efforts to obtain legislative protection for digital data.[265] Judicial consideration of third-party privacy practices merely recognizes that, in the absence of such legal obligations, a service provider may in some circumstances obtain a user's consent to law enforcement cooperation, provided that consent is genuine and robust. Where a service provider commits to protect a user's privacy, both with respect to other third parties generally and specifically with respect to the government, meanwhile, users ought to be entitled to take those commitments seriously—and expect their data to

[263] The features of robust and genuine consent to a law enforcement search identified in this Part touch on two of Richards and Hartzog's three "pathologies of digital consent." The third, incapacitated consent, may also arise where consumer genetics data is at issue. Where, for example, an individual obtains genetic sequence data for her child or another individual (other than herself), she may be engaging in consent that is incapacitated. See Richards & Hartzog, supra note 227, at 34 (defining "incapacitated consent" as consent "where voluntariness is simply not available as a matter of law, such as with children and others who are categorically incapable of legally consenting"). Moreover, incapacitated consent is likely to arise with respect to genetic relatives indirectly implicated by an individual's sharing of her genetic data with a consumer genetics platform. This matter is discussed in detail in a companion article.

[264] See, e.g., Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U.C. Davis L. Rev. 1183, 1186 (2016) (arguing for recognizing certain data intermediaries as "information fiduciaries," with attendant obligations to protect user privacy); Brennan-Marquez, supra note 67, at 649, 655 (arguing that many service providers should be recognized as "Fourth Amendment Fiduciaries," who are not free to disclose user information to the government, either voluntarily or by compulsion).

[265] See, e.g., California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 (West 2019) (providing consumers the right to request and receive access to personal information collected by businesses); Daisuke Wakabayashi, California Passes Sweeping Law to Protect Online Privacy, N.Y. Times (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html [https://perma.cc/TC39-TAFR] (reporting that California passed a digital privacy law that grants consumers greater control over their personal information online); Editorial Bd., Genetic-Testing Technology Is Progressing Rapidly. The Rules Need to Keep Up., Wash. Post (Sept. 4, 2018), https://www.washingtonpost.com/opinions/genetic-testing-technology-is-progressing-rapidly-the-rules-need-to-keep-up/2018/09/04/4a9baeee-9caa-11e8-b60b-1c897f17e185_story.html [https://perma.cc/J884-D4Q8] (arguing for Congress to create baseline standards and disclosure requirements to protect consumer data collected by genetic-testing companies).

remain secure from government use—and courts ought to hold police to those expectations.

IV. PRIVACY PRACTICES IN GENETIC GENEALOGY

In the wake of the alleged Golden State Killer's arrest, different consumer genetic platforms have adopted divergent responses to law enforcement use of their services. These responses span a wide gamut. Some services, including 23andMe and Ancestry, have consistently and explicitly denounced law enforcement use and vowed to oppose it. At least two others, GEDmatch and FamilyTreeDNA, have since welcomed law enforcement use, though both services have suffered from mismatches between their public-facing privacy statements and their internal practices along the way.

Together, the interaction of privacy practices and police access across these consumer genetic platforms helps to illuminate that such platforms can, indeed, be clear and explicit about their privacy practices—but also that such clarity is far from guaranteed. More specifically, the controversies stirred at both GEDmatch and FamilyTreeDNA due to quiet cooperation with law enforcement beyond the terms of each services' privacy practices demonstrate what consumer platforms ought not to do and courts ought not to validate. While both GEDmatch and FamilyTreeDNA now have in place privacy practices that better facilitate user consent than those in place before, both platforms continue to suffer from aspects of the "pathologies of digital consent."[266] Their missteps along the way, moreover, arguably undermine user, and judicial, confidence that the consent these platforms now facilitate is credible and enforceable.

One additional caveat is necessary: insofar as privacy policies, statements, and related practices may operate as consent to search, that consent may only be valid for those who engage directly with a particular platform. To be sure, genetic relatedness has been an integral aspect of police use of genealogical genetic databases thus far. In every reported arrest stemming from genealogical genetic data, the individual arrested was a genetic relative of the individual who shared genetic information with a third-party platform.[267] The issue of familial forensic identification is

[266] Richards & Hartzog, supra note 227.

[267] See, e.g., Jeff Hawkes & Tom Knapp, Raymond 'DJ Freez' Rowe Arrested for 1992 Killing of Schoolteacher Christy Mirack, Lancaster Online (June 25, 2018), https://lancaster-online.com/news/local/raymond-dj-freez-rowe-arrested-for-killing-of-schoolteacher-christy/-article_f05a2ee4-78b2-11e8-ad10-4382ef42f96d.html [https://perma.cc/EXK8-SY5X]

beyond the scope of this Article, however, and the subject of a companion article.[268]

A. Reinforced Expectations at 23andMe and Ancestry

Genetic services 23andMe and Ancestry are two of the largest providers of direct-to-consumer genetic sequencing. In the wake of the Golden State Killer arrest, each publicly disclaimed any connection to that investigation.[269] Indeed, as each service explained, it has a policy in place to minimize the likelihood that the government will make use of user genetic data. 23andMe explained bluntly, it's "our policy to resist law enforcement inquiries to protect customer privacy."[270] Meanwhile, AncestryDNA emphasized that it "advocates for its members' privacy and will not share any information with law enforcement unless compelled to by valid legal process."[271] In July 2018, 23andMe, Ancestry, and several other similar services publicly committed to more strongly advocate for and protect user genetic privacy within their own companies, in disclosing

(reporting that, in investigating the murder of Christy Mirack, the genealogical genetic match was "to a close Lancaster County relative of Rowe's"); Justin Jouvenal, The Unlikely Crime-Fighter Cracking Decades-Old Murders? A Genealogist., Wash. Post (July 16, 2018), https://www.washingtonpost.com/local/public-safety/in-decades-old-crimes-considered-all-but-unsolvable-genetic-genealogy-brings-flurry-of-arrests/2018/07/16/241f0e6a-68f6-11e8-bf8c-f9ed2e672adf_story.html [https://perma.cc/2F2Y-SM7A] ("The killer appeared to share enough DNA with two people to be second cousins."); Kyle Swenson, After 30 Years, Police Say They've Captured a Child-Killer Who Left a Sickening Trail of Taunts, Wash. Post (July 16, 2018), https://www.washingtonpost.com/news/morning-mix/wp/2018/07/16/i-been-watching-you-a-child-killer-taunted-little-girls-with-terrifying-notes-police-say-after-30-years-dna-led-to-an-arrest [https://perma.cc/37D7-A32R] (reporting that, in investigating the murder of Ashley Tinsley, Parabon "was able to narrow the possible suspects down to two brothers in the Fort Wayne area").

[268] See Ram, supra note 48. In brief, there is good reason to believe that *Carpenter* will bolster claims that familial forensic identification violates the Fourth Amendment. Most significantly, *Carpenter* provides a foundation for a claim that an individual may have an expectation of privacy in information that is informative about her, even if it resides formally in the property of another. See Carpenter v. United States, 138 S. Ct. 2206, 2235 (Kennedy, J., dissenting) (2018) (criticizing the Court for concluding that there was a Fourth Amendment search where "the Government did not search anything over which Carpenter could assert ownership or control"); id. at 2269–70 (Gorsuch, J., dissenting) ("I doubt that complete ownership or exclusive control of property is always a necessary condition to the assertion of a Fourth Amendment right.").

[269] See Wagstaff, supra note 17 ("Spokespeople from 23andMe and Ancestry said the companies were not involved in the DeAngelo case.").

[270] Id.

[271] Id.

their users' genetic data to other third parties, and in responding to law enforcement requests.[272]

The terms of use and privacy policies of these institutions back up those public commitments. The terms of service at 23andMe explicitly prohibit law enforcement from using the service for crime detection purposes, requiring users to "agree not to . . . use any information received through the Services to attempt to identify other customers, to contact other customers (other than through features for contacting other users such as DNA Relatives offered pursuant to the Services), or *for any forensic use*."[273] 23andMe's privacy policy, meanwhile, makes clear that individual-level data stays within the walled garden of the 23andMe community, absent additional consent. In the Privacy Highlights that summarize the most essential provisions of the service's full privacy policy, 23andMe promises not to "sell, lease, or rent your individual-level information to any third party or to a third party for research purposes without your explicit consent."[274] More specifically, 23andMe explains that it does not "share customer data with any *public databases*," "provide any person's data (genetic or non-genetic) to an *insurance company* or *employer*," or "provide information to *law enforcement* or *regulatory authorities* unless required by law to comply with a valid court order, subpoena, or search warrant for genetic or Personal Information."[275]

Ancestry similarly invites users to reasonably believe that their genetic data is secure from prying government eyes. In the introductory paragraphs of its terms and conditions, Ancestry explains, "Your privacy is very important to us."[276] "In particular," Ancestry emphasizes, "you

[272] See Future of Privacy Forum, supra note 261, at 7–9; Carson Martinez, Privacy Best Practices for Consumer Genetic Testing Services, Future of Privacy Forum (July 31, 2018), https://fpf.org/2018/07/31/privacy-best-practices-for-consumer-genetic-testing-services/ [https://perma.cc/4CU7-CAER] (summarizing the report and identifying "23andMe, Ancestry, Helix, MyHeritage, and Habit" as participants).

[273] "23andMe" Terms of Service, supra note 197 (emphasis added) (identifying "Customer Conduct - Unlawful and Prohibited Use"). Other direct-to-consumer DNA platforms include similar terms. See Terms and Conditions, MyHeritage, https://www.myheritage.com/FP/-Company/popup-terms-conditions.php [https://perma.cc/S2RE-P57M] (last visited Aug. 29, 2019); Terms of Service, LivingDNA (July 2018), https://livingdna.com/privacy-centre/terms [https://perma.cc/L8S3-EWZB] ("You undertake, promise, warrant and agree . . . [n]ot to use the results of our DNA ancestry test that we provide to you for any purpose other than for ancestry research . . . .").

[274] "23andMe" Privacy Highlights, supra note 257 (describing "Access To Your Information").

[275] Id.

[276] Ancestry Terms and Conditions, supra note 196.

should be aware that we do not share your Genetic Information . . . with employers, insurance providers, or third-party marketers without your consent, and will *not share your Genetic Information with law enforcement* unless compelled by valid legal process as described in our Privacy Statement."[277] Like 23andMe, Ancestry requires its users to confirm that "[a]ny saliva sample you provide is either your own or the saliva of a person for whom you are a parent or legal guardian," thus excluding samples submitted by law enforcement from the scope of valid—and expected—sources of DNA.[278] Ancestry's privacy policy reiterates many of these statements.[279]

These invitations to rely on 23andMe or Ancestry to protect one's privacy are not merely hidden in the minutiae of each service's long and detailed policies. Rather, in both instances, these privacy practices are plainly and explicitly disclosed on prominent pages of their respective websites. On 23andMe's homepage, questions answered at the bottom of the page include "How is my privacy protected?"[280] In response, 23andMe states, "[w]e will not share your individual-level information with any third party without your explicit consent," and "[w]e do not provide information to law enforcement unless we are required to comply with a valid subpoena or a court-ordered request."[281] Ancestry's homepage contains a similar "Top questions about AncestryDNA," including "[h]ow secure and private is AncestryDNA?"[282] In response, Ancestry reiterates, "[y]our privacy is important to us," and "[w]e do not share with third parties your name or other common identifying information linked to your genetic data, except as legally required or with your explicit consent."[283] Ancestry's Privacy Philosophy page similarly emphasizes "[y]our trust is our top priority," and in response to the question "Does Ancestry respond to law enforcement requests?," explains that "[f]or all requests, Ancestry requires valid legal process in writing before producing any personal information about our users."[284]

[277] Id. (emphasis added).
[278] Id. (under "Important Things for You to Understand When You Use Our Services").
[279] Your Privacy, Ancestry, supra note 119.
[280] 23andMe, https://www.23andme.com/ [https://perma.cc/AEC9-FZ2Q] (last visited July 17, 2019).
[281] Id.
[282] Ancestry, https://www.ancestry.com/dna/ [https://perma.cc/W2G4-JQZB] (last visited July 17, 2019).
[283] Id.
[284] Ancestry Privacy Philosophy, supra note 196.

Both sites publish a Transparency Report as well, disclosing the number of government requests for user data it has received. Once again, 23andMe's Transparency Report invites users to rely on the company not to disclose user genetic data unnecessarily: "Respect for customer privacy and transparency are core principles that guide 23andMe's approach to responding to legal requests and maintaining customer trust."[285] 23andMe assures users that "we will closely scrutinize all law enforcement and regulatory requests and we will only comply with court orders, subpoenas, search warrants or other requests that we determine are legally valid."[286] Ancestry's Transparency Report once again insists, "[y]our privacy is our top priority," and explains, "Ancestry requires valid legal process in order to produce information about our members."[287]

These privacy protection standards are also clearly laid out for law enforcement specifically in a Guide for Law Enforcement on each site. Ancestry informs interested law enforcement officers, "any data relating to the DNA of an Ancestry user will be released only pursuant to a valid search warrant from a government agency with proper jurisdiction."[288] 23andMe's policy is similarly clear, explaining that "23andMe chooses to use all practical legal and administrative resources to resist requests from law enforcement, and we do not share customer data with any public databases, or with entities that may increase the risk of law enforcement access."[289] 23andMe further informs law enforcement personnel, "[u]se of the 23andMe Personal Genetic Service for casework and other criminal investigations falls outside the scope of our services intended use."[290]

To be sure, both 23andMe and Ancestry reserve the authority to use or disclose user genetic data in various ways. Most significantly, both companies' policies expressly contemplate the disclosure of user genetic data in "aggregate" form intended not to be individually identifiable.[291] That

[285] Transparency Report, 23andMe (July 15, 2019), https://www.23andme.com/transparency-report/ [https://perma.cc/AW4V-9TQ9].

[286] Id.

[287] Ancestry 2018 Transparency Report, Ancestry (Dec. 31, 2018), https://www.ancestry.com/cs/transparency [https://perma.cc/NVE8-PEHZ].

[288] Ancestry Guide for Law Enforcement, Ancestry, https://www.ancestry.com/cs/legal/lawenforcement/ [https://perma.cc/AHP8-WWHG] (last visited July 17, 2019).

[289] 23andMe Guide for Law Enforcement, supra note 18.

[290] Id. (under "Use of 23andMe Personal Genetic Service for Law Enforcement Casework and Forensics").

[291] Full Privacy Statement, 23andMe (July 17, 2018), https://www.23andme.com/about/privacy/ [https://perma.cc/M5MA-RJM6] ("We may share Aggregate Information, which is information that has been stripped of your name and contact information and combined with

is in many ways central to their business plans. For instance, in 2018, GlaxoSmithKline entered into an agreement to acquire a $300 million stake in 23andMe in order to gain access to the millions of 23andMe customers who have agreed to allow their "de-identified" genetic data to be used for research purposes.[292] In 2015, 23andMe similarly partnered with Pfizer and Genentech, with Genentech paying more than $60 million.[293]

Yet, consent to disclosure of one's data aggregated with the data of others ought not amount to consent to law enforcement use of one's individual-level genetic profile. As the Court in *Carpenter* observed, cell phone companies similarly share or sell aggregate user data, including cell site location information.[294] This did not undermine Carpenter's expectation of privacy in his location data or amount to consent for the police to use it,[295] and it similarly should not undermine or waive an expectation of privacy in one's genetic data.

In sum, 23andMe and Ancestry have articulated a commitment to user genetic privacy that is explicit, visible, and understandable. They plainly invite users to expect that their genetic privacy will be maintained, at least with respect to their individual-level data. Such privacy practices cannot amount to consent to government search of the database—instead, it reinforces users' well-founded expectations of privacy in their genetic data.

These policies are not without flaws, of course. As set forth above, they leave unchecked the sharing of broad swaths of aggregate genetic data with non-law enforcement third parties, including pharmaceutical

information of others so that you cannot reasonably be identified as an individual, with third parties."); id. ("23andMe Research uses Aggregate and/or Individual-level Genetic Information and Self-Reported Information as specified in the appropriate Consent Document(s) . . . ."); Your Privacy, Ancestry, supra note 119 ("Ancestry may disclose user information in an aggregated form as part of the Services or our marketing, or in scientific publications published by us or our research partners. . . . Such disclosure will never include Personal Information."). Additional terms of service or privacy practices related to the research use of genetic data are not discussed in this Part, as both 23andMe and Ancestry require additional consent or authorization to share customer data with research partners or for research purposes.

[292] Jamie Ducharme, A Major Drug Company Now Has Access to 23andMe's Genetic Data. Should You Be Concerned?, Time (July 26, 2018), http://time.com/5349896/23andme-glaxosmith-kline/ [https://perma.cc/HJW4-ENCY].

[293] Megan Molteni, 23andMe Is Digging Through Your Data for a Parkinson's Cure, Wired (Sept. 13, 2017, 7:00 AM), https://www.wired.com/story/23andme-is-digging-through-your-data-for-a-parkinsons-cure/ [https://perma.cc/4YF7-S4JB].

[294] See Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018).

[295] Id. at 2223.

companies.[296] Although the relevant privacy policies purport to limit this sharing to data that is not traceable to an identifiable individual, such assurances are difficult to take at face value in light of the growing body of research indicating that genetic data is perpetually identifiable.[297] Nonetheless, these policies reasonably lead users to have confidence in the privacy of their personally identifiable genetic data—notwithstanding scientific realities. Accordingly, these practices should reinforce, rather than waive, expectations of privacy in the identifiable data held by firms like 23andMe and Ancestry.

B. Likely Consent to Search at GEDmatch (at Least in Part)

While 23andMe and Ancestry take pains to emphasize their commitment to user genetic privacy, particularly vis-a-vis the government, GEDmatch has taken quite the opposite approach. Through successive iterations of its site policy and web portal announcements, GEDmatch has attempted to secure its users' consent to law enforcement access to their genetic data. This Section charts these iterations of GEDmatch's privacy practices since forensic genetic genealogy burst into public consciousness, identifying ways in which GEDmatch has improved the consent it secures for law enforcement access, while noting flaws still present.

Prior to the arrest of the alleged Golden State Killer, GEDmatch's site policy informed users, "[I]f you require absolute privacy and security, we must ask that you do not upload your data to GEDmatch. If you already have it here, please delete it."[298] That policy elaborated further, informing users that "[w]hile the results presented on this site are intended solely for genealogical research, we are unable to guarantee that users will not find

[296] See supra notes 291–293 and accompanying text.

[297] See, e.g., Yaniv Erlich et al., Re-Identification of Genomic Data Using Long Range Familial Searches 1, 3 (June 18, 2018) (unpublished manuscript), https://www.biorxiv.org/content/biorxiv/early/2018/06/19/350231.full.pdf [https://perma.cc/AM83-JCKF] (finding that a long-range familial search of a database of 600,000 people has a forty-six percent chance of returning a third cousin or closer relative); Amy L. McGuire & Richard A. Gibbs, No Longer De-Identified, 312 Sci. 370, 370 (2006) (observing that "an individual can be uniquely identified with access to just 75 single-nucleotide polymorphisms (SNPs) from that person," while "[g]enomewide association studies routinely use more than 100,000 SNPs to genotype individuals" (citing Zhen Lin et al., Genomic Research and Human Subject Privacy, 305 Sci. 183, 183 (2004))); Ram, supra note 9, at 886–87 nn.82–84 (collecting sources demonstrating genomic re-identification).

[298] GEDmatch.Com Terms and Policy Statement, GEDmatch (Aug. 18, 2017), https://web.archive.org/web/20180427203335/https://www.gedmatch.com/policy.php [https://perma.cc/J5AG-943L] (under "Privacy").

other uses. If you find the possibility unacceptable, please remove your data from this site." Nonetheless, GEDmatch also explained, "It is our policy to never provide your genealogy, DNA information, or email address to 3rd parties, except as noted above."[299]

This first iteration of GEDmatch's privacy practices almost certainly would not satisfy the requirements for valid and enforceable consent to government search set out above.[300] For one thing, a privacy policy, standing alone, is unlikely to give rise to knowing and voluntary consent.[301] For another, before the arrest of the alleged Golden State Killer, it is unlikely that site users would have associated "other uses" of genetic data with "law enforcement uses."[302]

Nor is it sufficient to reject privacy claims at GEDmatch due to the structure of the site itself. Although journalists and others have described GEDmatch as "a public database open to anyone,"[303] that is not quite right. To be sure, unlike 23andMe and Ancestry, which require users to submit a sizeable saliva sample for analysis and sequencing,[304] GEDmatch does not sequence anything. Rather, GEDmatch enables users of other genetic sequencing services to share their genealogical data with one another through its single platform.[305] Users upload genetic sequence data developed elsewhere to GEDmatch, where it is compressed in a proprietary format.[306] GEDmatch provides its platform largely free of charge.[307]

[299] Id.

[300] See supra Section III.B.

[301] See supra notes 250–256 and accompanying text (describing the limited role that privacy policies and similar documents, standing alone, may play in garnering valid user consent).

[302] See Richards & Hartzog, supra note 227, at 26 (explaining that "[u]nwitting consent" includes consent where "consumers might not understand the consequences or risks of the informational relationship"); id. at 40 (arguing that digital consent is most likely to be valid when, inter alia, the risks of that consent are vivid and easily understood); supra notes 104–107 and accompanying text.

[303] Sarah Zhang, How a Tiny Website Became the Police's Go-To Genealogy Database, Atlantic (June 1, 2018), https://www.theatlantic.com/science/archive/2018/06/gedmatch-police-genealogy-database/561695/ [https://perma.cc/GM7V-WRF9].

[304] Providing Your Saliva Sample, supra note 41 ("The recommended volume of saliva to provide is about 2 mL, or about ½ teaspoon."); Taking an Ancestry DNA Test supra note 41 (providing advice for what to do "[i]f you can't produce enough saliva in one try").

[305] GEDmatch Terms and Policy Statement, supra note 298 (under "Security").

[306] See id.

[307] See GEDmatch, supra note 188 ("Some applications are free. More advanced applications require [a paying] membership. . . .").

But this structure does not yield a fully open architecture. Every user must create an account through which to upload their own genetic data for genealogical matching purposes.[308] GEDmatch also "take[s] steps to prevent your Genealogy Data from being available to the casual web surfer or to the search engines (e.g. Google)."[309] Moreover, as GEDmatch's own site policy changes in response to the Golden State Killer arrest and as subsequent investigations demonstrate, GEDmatch could have adopted an explicit prohibition of law enforcement use of its platform (or a broader prohibition on use for purposes other than traditional genealogical research) from the outset.[310]

It did not. Instead, shortly after police disclosed that investigators had used the GEDmatch platform in the Golden State Killer investigation, GEDmatch made its first attempts to secure explicit user consent to law enforcement access. Within days, GEDmatch posted a notice to users on its homepage that they should have expected such use: "Although we were not approached by law enforcement or anyone else about this case or about the DNA, it has always been GEDmatch's policy to inform users that the database could be used for other uses, as set forth in the Site Policy."[311] The notice emphasized that, although GEDmatch "was created for genealogical research, it is important that GEDmatch participants understand the possible uses of their DNA, including identification of relatives that have committed crimes or were victims of crimes."[312] In other words, GEDmatch embraced law enforcement's use of its genetic data for crime detection purposes.

When GEDmatch updated its site policy less than a month after the Golden State Killer arrest, moreover, that embrace became even more explicit. The updated policy newly enumerated specific categories of genetic data that were acceptable for upload, requiring users to "agree that you will not upload Raw [Genetic] Data that does not satisfy one of these

[308] See id.

[309] GEDmatch.com Terms of Service and Privacy Policy, supra note 20.

[310] See GEDmatch.com Terms of Service and Privacy Policy, GEDmatch (May 18, 2019), https://www.gedmatch.com/tos.htm [https://perma.cc/4W3V-BUSR] (explaining that genetic profiles "identified as being uploaded for Law Enforcement purposes will only be matched with [profiles] that have 'opted-in'" to such use).

[311] See Taylor Hatmaker, DNA Analysis Site that Led to the Golden State Killer Issues a Privacy Warning to Users, TechCrunch (Apr. 27, 2018) (quoting User Homepage, GEDmatch (last visited Oct. 2, 2019) (on file with Virginia Law Review Association)), https://techcrunch.com/2018/04/27/golden-state-killer-gedmatch/ [https://perma.cc/HM6W-2EVF].

[312] Id.

categories."[313] One of those categories was "DNA obtained and authorized by law enforcement to . . . identify a perpetrator of a violent crime against another individual."[314] The policy went on to define "[v]iolent crime" as "homicide or sexual assault."[315] GEDmatch required all users to agree to the revised terms of service anew.

This set of privacy practices appeared clear, concise, and unmistakable—key hallmarks for valid consent—until GEDmatch itself undermined it. Despite limiting law enforcement access to homicide and sexual assault crimes, in late 2018, GEDmatch's site operators privately authorized law enforcement to utilize the GEDmatch database to investigate a different crime.[316] Although the crime in question, an aggravated assault, was a serious one, it nonetheless plainly fell outside the scope of any consent that GEDmatch had secured from its users.[317]

Moreover, although police are typically not constitutionally constrained only to investigate a particular crime once they have obtained consent to search, deceptive tactics can raise Fourth Amendment concerns.[318] At least for investigating crimes other than homicide or sexual assault, GEDmatch failed to secure its users' consent.[319]

Most recently, in May 2019 and in response to outcry about its derogation from its own privacy practices, GEDmatch altered those practices once again. In a dramatic change, GEDmatch made all existing genetic profiles *un*available for law enforcement use, while permitting users

[313] GEDmatch.com Terms of Service and Privacy Policy, supra note 20 (under "Raw DNA Data Provided to GEDmatch").

[314] Id.

[315] Id.

[316] See Aldhous, supra note 22.

[317] See id. The assault in question involved an "assailant who broke into a Mormon church on Nov. 17, 2018, and put a 71-year-old woman who was playing the organ in a chokehold. She passed out several times, according to a police press release, but survived the attack." Id. In justifying the decision to permit investigators to search the GEDmatch database in this case, GEDmatch's operator Curtis Rogers stated, "This case was as close to a homicide as you can get," while Parabon NanoLabs' CEO explained, "In this particular incident, the police made a compelling case that this person was a public risk." Id.

[318] See Kiel Brennan-Marquez & Peter Siegelman, Reconceptualizing Police Deception, 4–5 (unpublished manuscript) (on file with author) (analyzing the circumstances under which police deception in securing consent to search renders that consent unconstitutional and invalid).

[319] See, e.g., Florida v. Jardines, 569 U.S. 1, 9 (2013) ("The scope of a license—express or implied—is limited not only to a particular area but also to a specific purpose. Consent at a traffic stop to an officer's checking out an anonymous tip that there is a body in the trunk does not permit the officer to rummage through the trunk for narcotics.").

affirmatively to opt their data back in for such use.[320] In bold, red text at the top of the user home page, once a user has logged in to her account, GEDmatch now explains:

> On May 18, GEDmatch changed its rules relating to matches with kits uploaded by representatives of Law Enforcement. All previously existing DNA kits in the GEDmatch database were set to 'opt-out' of these comparisons. This change affects searches for unknown bodies and violent crimes. If you wish to include your kit in these searches, you need to click on the 'Police' icon to the right of your kit number on this page. If your kit was previously marked as 'Research', you will need to use the 'Pencil' icon to opt-in.[321]

The site's terms of service reflect concordant changes, also demarcated (for now) in highly-visible red text explaining, "There are 4 classes of DNA data on this Site: 'Private', 'Research', 'Public + opt-in' and 'Public + opt-out.'"[322] The terms of service explain further that "Public + opt-in" data "is available for comparison to any Raw Data in the GEDmatch database using the various tools provided for that purpose," while "Public + opt-out" data is "is available for comparison to any Raw Data in the GEDmatch database, except DNA kits identified as being uploaded for Law Enforcement purposes."[323]

At the same time, GEDmatch expanded the scope of crimes that law enforcement may investigate using GEDmatch data to include "murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault."[324] And it actively encourages users to opt in for law enforcement access, declaring in bold, blue text on the user home page, "We encourage everybody to [opt in to law enforcement access], unless you have specific reasons not to do so. There are thousands of families depending on

[320] See GEDmatch Tools for DNA and Genealogy Research, GEDmatch, https://www.gedmatch.com/select.php (last visited Sept. 10, 2019) (on file with Virginia Law Review Association).

[321] Id.

[322] GEDmatch.com Terms of Service and Privacy Policy, supra note 20 (under "DNA Data").

[323] Id. Although law enforcement could, as a practical matter, misrepresent the nature and source of genetic data they wish to compare to GEDmatch user data, and thus upload crime scene DNA to the general "Public + opt out" database, there would be little arguable basis for concluding that users in that database had consented to law enforcement use of their genetic data. In the absence of such consent, law enforcement access to this genetic data would run afoul of users' reasonable expectation of privacy in their genetic data. See supra Part II.

[324] Id. (under "Raw DNA Data Provided to GEDmatch").

GEDmatch for closure to terrible tragedies."[325] The site even links to a video testimonial in which a family member of a victim of the Golden State Killer emphasizes the importance of opting in.[326] As of July 2, 2019, GEDmatch users have opted in roughly 85,000 genetic profiles for law enforcement use.[327]

Taken together, these changes do a great deal to facilitate robust and genuine consent from existing GEDmatch users. Although GEDmatch encourages existing users to make their data accessible for law enforcement searches, it has not over-weighted that preference by making user data accessible by default.[328] Moreover, by requiring existing users to engage in affirmative conduct to make their data available for law enforcement use, GEDmatch has enhanced the probability that participating users will have that status both knowingly and voluntarily.[329] At least for existing users, GEDmatch has created privacy practices surrounding law enforcement access that are at least as explicit, visible, and understandable as are 23andMe and Ancestry's countervailing commitments to user genetic privacy. In other words, for existing GEDmatch users who have consented—by opting in—to law enforcement access, that consent likely satisfies the requirements for consent to a Fourth Amendment search.

Unfortunately, the same cannot be said for new users to GEDmatch. Despite embracing the description of "an opt-out default for law enforcement matching,"[330] that language appears to be accurate only with respect

[325] See GEDmatch Tools for DNA and Genealogy Research, GEDmatch, https://www.gedmatch.com/select.php (last visited Aug. 21, 2019) (on file with Virginia Law Review Association).

[326] Id.; Debra Dee, Upload Your DNA to GEDmatch.com & Opt In!, YouTube (May 31, 2019), https://www.youtube.com/watch?v=PlbfAYVtnq8&feature=youtu.be [https://perma.cc/DV6D-6EHA].

[327] See Hautala, supra note 3 ("Users have opted back in about 85,000 of the site's more than 1 million kits so far.").

[328] See Ram & Roberts, supra note 3 (arguing that adopting a default status of law enforcement access arrogates decision-making power from user to platform).

[329] See Richards & Hartzog, supra note 227, at 29–30 (explaining that tying consent to use a service at all can constitute coerced consent). To be sure, separating consent to law enforcement access from agreement to use GEDmatch at all proliferates the opportunities for consent, something that Richards and Hartzog criticize. See id. at 37–39. Richards and Hartzog argue that, to best achieve knowing and voluntary consent, there must be "infrequent requests" for consent all together. Id. at 37. Nonetheless, as between coerced consent through platform use and separate consent for law enforcement access, the latter seems preferable.

[330] Family History Fanatics, Your DNA Can Help Law Enforcement—A Segment of DNA, YouTube (May 21, 2019), https://www.youtube.com/watch?v=FiiKfruIvcE&feature=youtu.be [https://perma.cc/G39J-2EBC] (stating that GEDmatch has changed to automatic opt-out for law enforcement matching at two seconds into the video); see GEDmatch Tools for DNA

to pre-existing GEDmatch genetic profiles, as discussed above. New users face a different—and more unwitting—process for consent to law enforcement use. Users who seek to upload new genetic data to the GEDmatch database are presented with "privacy options" in which the option including law enforcement access (labeled "Opt-in") appears pre-selected by default.[331] These users, in other words, are presumed to have consented to law enforcement use of their genetic data and must take affirmative steps to escape such use. In adopting the language of an "opt-in policy" while actually creating an opt out approach for new profiles, GEDmatch further muddies the waters, undermining confidence that any consent secured for new profiles can be knowing and voluntary—and worthy of judicial recognition.[332]

In sum, GEDmatch has, from the first, attempted to articulate and embrace a commitment to share user data with law enforcement specifically. Over time, that commitment has become more explicit, visible, and understandable, and the means of securing user consent to such sharing has become more robust. Today, existing users who have affirmatively opted in to law enforcement matching reasonably should know that law enforcement may—and likely will—compare it to genetic data extracted from crime scene samples. That consent to law enforcement access may properly inform Fourth Amendment analysis.[333] Similarly, existing users who have declined to opt in to law enforcement matching should be able to reasonably rely on GEDmatch to ensure that law enforcement access does not occur. In this way, privacy practices act not only as a shield but also as a hand, assisting law enforcement to access what might otherwise have been private data. Yet the rocky path that GEDmatch's site changes have charted, the behind-the-scenes facts that prompted them, and the still-unwitting consent they facilitate for new profiles tempers the confidence that users, and courts, may have in the knowing and voluntary nature of any consent at GEDmatch. Thus, consent to law enforcement access through GEDmatch, for now, may only be arguable at best.

and Genealogy Research, supra note 325 (linking text stating "New Click here to see video on GEDmatch and Law Enforcement Matching" to the Family History Fanatics video).

[331] See GEDmatch Raw DNA Upload Utility, supra note 25.

[332] Cf. Ram & Roberts, supra note 3 (describing how opt-in and opt-out defaults are "sticky" and can significantly affect decision making and outcomes); Richards & Hartzog, supra note 227, at 21 (observing that unwitting consent can occur where consent practices "switch from 'opt out' to 'opt in' options in a series of choices").

[333] See supra Section II.B.

C. Questionable Consent to Search at FamilyTreeDNA

Until January 2019, FamilyTreeDNA was regarded as one of the most privacy-protective consumer genetics companies. Its homepage prominently promised, "We won't share your DNA."[334] The service was also a supporter of the Future of Privacy Forum's Privacy Best Practices, which require "[v]alid legal process for the disclosure of Genetic Data to law enforcement."[335] And FamilyTreeDNA had recently been honored as the best consumer genetic service for privacy.[336]

Yet, for nearly a year, FamilyTreeDNA had been working with the FBI to analyze crime scene DNA samples and compare them to the other genetic profiles in its database.[337] The news report about an information sharing agreement between FamilyTreeDNA and the FBI caught the genealogy community, and the public at large, by surprise.[338] The initial news report in Buzzfeed was repeated on dozens of other news sites.[339] The Future of Privacy Forum promptly removed FamilyTreeDNA from its list of supporters of the Privacy Best Practices.[340] And FamilyTreeDNA hastily issued a letter to users apologizing for its poor

[334] FamilyTreeDNA, https://www.familytreedna.com (last visited Aug. 22, 2019).

[335] Future of Privacy Forum, supra note 261.

[336] See Brad Berman, Best DNA Testing Kits, U.S. News (Jan. 7, 2019), https://health.usnews.com/wellness/articles/2019-01-07/best-dna-testing-kits [https://perma.cc/WZ2S-LXPN] (naming FamilyTreeDNA the "Best for Genealogical Research and Strict Privacy"); Dieter Holger, Best DNA Testing Kits: Discover the Secrets Stored in Your Genes, PCWorld (Feb. 12, 2019), https://www.pcworld.com/article/3317567/best-dna-kits.html [https://perma.cc/JB4U-NEGF] (naming FamilyTreeDNA the "Best DNA kit for privacy" and explaining that "Family Tree DNA [sic] doesn't ask you to consent to any agreements that might result in your genetic data ending up in the hands of companies or researchers").

[337] See Marcus, supra note 29; Hernandez, supra note 29.

[338] See, e.g., Nick Natario, Houston Based DNA Testing Company Defends Decision to Allow Police to Access Results, ABC13 Eyewitness News (Feb. 8, 2019), https://abc13.com/society/familytreedna-defends-decision-to-allow-police-to-access-results/5128335/ [https://perma.cc/DUE8-6W7B].

[339] See, e.g., Kristen V. Brown & Bloomberg, A Major DNA-Testing Company Is Sharing Some of Its Data with the FBI. Here's Where It Draws the Line, Fortune (Feb. 2, 2019), http://fortune.com/2019/02/01/genetic-testing-consumer-dna-familytreedna-fbi/ [https://perma.cc/F6YK-HM42]; Dan Robitzski, This DNA Testing Company Gave Its Data to the FBI, Futurism (Feb. 1, 2019), https://futurism.com/dna-testing-data-fbi [https://perma.cc/DDY5-Y5WF].

[340] See Future of Privacy Forum, supra note 261 (listing, and then striking out, FamilyTreeDNA from the list of supporters of the Privacy Best Practices).

communication and defending its decision to permit law enforcement to seek matches in its database of user genetic profiles.[341]

In that letter, FamilyTreeDNA President Bennett Greenspan explained that users should have expected law enforcement to make use of the FamilyTreeDNA database.[342] After all, such use was purportedly consistent with FamilyTreeDNA's then-existing Terms of Service. In May 2018, to comply with the European Union's General Data Protection Regulation, FamilyTreeDNA notified users about an update to its Terms of Service.[343] Those updated Terms stated that FamilyTreeDNA services must not be used "for any law enforcement purposes, forensic examinations, criminal investigations, and/or similar purposes without the required legal documentation and written permission from FamilyTreeDNA."[344] FamilyTreeDNA's Privacy Statement, meanwhile, was largely silent about sharing user data with law enforcement, apart from a standard disclosure that the service would share a user's "Personal Information" when compelled to do so.[345]

To be sure, for a brief period between December 2018 and February 2019, FamilyTreeDNA's Terms of Service included language much like that used by GEDmatch.[346] This language required users to agree not to use FamilyTreeDNA services "for law enforcement purposes" unless the DNA at issue "was obtained and authorized by law enforcement to either: (1) identify a perpetrator of a violent crime, as defined in 18 U.S. Code

[341] See Bennett Greenspan, A Letter to Our Customers, FamilyTreeDNA (Feb. 3, 2019), https://mailchi.mp/familytreedna/letter-to-customers?e=[UNIQID] [https://perma.cc/9G4J-9REW].

[342] See id.

[343] Id.

[344] Id.; see Terms of Service, FamilyTreeDNA (Feb. 3, 2019) [hereinafter FamilyTreeDNA Febuary 2019 Terms of Service], https://www.familytreedna.com/legal/terms-of-service/031-22019 [https://perma.cc/R23F-NTN3] (under "Requirements for Using the Services" in Section 6.B.xii); Terms of Service, FamilyTreeDNA (May 22, 2018), https://www.familytreedna.com/legal/terms-of-service/12182018 [https://perma.cc/8F4C-V7X4] (same).

[345] FamilyTreeDNA Privacy Statement, FamilyTreeDNA [hereinafter FamilyTreeDNA pre-March 2019 Privacy Statement], https://www.familytreedna.com/legal/privacy-statement/03122019 [https://perma.cc/WY8T-BKHH] (last visited Aug. 23, 2019) (describing in Section 5.D the circumstances under which FamilyTreeDNA will allow "law enforcement" access to user information "[f]or Legal or Regulatory Process").

[346] Terms of Service, FamilyTreeDNA (Dec. 18, 2018) [hereinafter FamilyTreeDNA December 2018 Terms of Service], https://www.familytreedna.com/legal/terms-of-service/02032019 [https://perma.cc/NTG5-L2ZC] (under "Requirements for Using the Services" in Section 6.B.xii); FTDNA Opens the Door to the Cops, DNA Geek (Jan. 31, 2019), https://thednageek.com/ftdna-opens-the-door-to-the-cops/ [https://perma.cc/PT2C-86HH].

§ 924(e)(2)(B), against another individual, including sexual assault, rape, and homicide; or (2) identify the remains of a deceased individual."[347] Unlike GEDmatch, however, FamilyTreeDNA did not notify users about this change in the Terms of Service.[348] Indeed, once users and the public actually became aware of this change, FamilyTreeDNA reverted to the prior, GDPR-compliant version of the Terms of Service from May 2018.[349]

On this record, it is simply not the case that FamilyTreeDNA users knowingly or voluntarily consented to repeated law enforcement use of their genetic data to generate leads in criminal investigations. At best, the site's Terms of Service reserved to FamilyTreeDNA the ability to permit law enforcement use of its service with "the required legal documentation and written permission from FamilyTreeDNA."[350] But there has been no indication that the FBI or other law enforcement agencies have ever presented FamilyTreeDNA with a subpoena or other order that might satisfy a requirement for "legal documentation." Rather, FamilyTreeDNA appeared to rest its sharing policy on the Terms of Service's requirement of "written permission."[351] That much was clear from FamilyTreeDNA's February 2019 letter to users, which explained that the Terms of Service "require[] law enforcement to receive our permission to enter the database."[352] Requiring only permission, and not legal documentation, however, was arguably inconsistent with the Terms of Service themselves, which utilized the word "and" between these requirements for law enforcement use.[353]

[347] See FamilyTreeDNA December 2018 Terms of Service, supra note 346, § 6.B.xii.

[348] Greenspan, supra note 341 ("Without infringing upon our customers' privacy, the language in the paragraph referring to law enforcement was updated in December, although nothing changed in the actual handling of such requests. It was an oversight that notice of the revision was not sent to you and that is our mistake."); see FTDNA Opens the Door to the Cops, supra note 346.

[349] Greenspan, supra note 341 ("[W]e are reverting our TOS to our May 2018 version, and any future changes will be communicated to you in a timely manner."); see FamilyTreeDNA Febuary 2019 Terms of Service, supra note 344, § 6.B.xii.

[350] FamilyTreeDNA February 2019 Terms of Service, supra note 344, § 6.B.xii.

[351] Id. (providing in Section 6.B.xii that law enforcement use of FamilyTreeDNA is not permitted "without the required legal documentation and written permission from FamilyTreeDNA"); see Greenspan, supra note 341.

[352] Greenspan, supra note 341.

[353] See, e.g., 1A Norman J. Singer, Statutes and Statutory Construction § 21:14 (6th ed. 2002) ("Where two or more requirements are provided in a section and it is the legislative intent that all of the requirements must be fulfilled in order to comply with the statute, the conjunctive 'and' should be used. Statutory phrases separated by the word 'and' are usually

Moreover, FamilyTreeDNA's Terms of Service implied that law enforcement use would be an exceptional circumstance, rather than a pattern of permission. The requirements for permitting law enforcement use followed a statement that the FamilyTreeDNA service generally must not be used "for any law enforcement purposes, forensic examinations, criminal investigations, and/or similar purposes."[354] The site's Privacy Statement, meanwhile, did not mention at all a voluntary program of cooperation with law enforcement to investigate criminal cases.[355]

Thus, for nearly a year, FamilyTreeDNA gave users only the barest of signals that it would be cooperating with law enforcement to analyze and compare crime scene DNA to user DNA on a regular basis. That signal was further muted in light of the fact that it came, if at all, buried in the site's long, abstruse Terms of Service. In this way, FamilyTreeDNA's early embrace of law enforcement access was quite unlike even GEDmatch's initial cooperation with law enforcement, which was the subject of highly visible statements and notices to users.[356]

Perhaps recognizing the mismatch between its user-facing privacy practices and its internal conduct, in March 2019, FamilyTreeDNA reformed its Terms of Service, Privacy Policy, and user agreements to match more closely its actual practices. FamilyTreeDNA also introduced a law enforcement matching option separate from other site uses, months before GEDmatch did the same.[357] Together, these changes in privacy practices purport to authorize law enforcement to seek matches with nearly all users to investigate "homicide, abduction, or sexual assault" crimes.[358]

---

to be interpreted in the conjunctive. Where a failure to comply with any requirement imposes liability, the disjunctive 'or' should be used." (footnotes omitted)); Jacob Scott, Codified Canons and the Common Law of Interpretation, 98 Geo. L.J. 341, 357 (2010) (observing the "[c]ommon grammar canon[]" regarding the different meanings of "and" and "or").

[354] FamilyTreeDNA Febuary 2019 Terms of Service, supra note 344, § 6.B.xii.

[355] FamilyTreeDNA pre-March 2019 Privacy Statement, supra note 345. Indeed, prior to the March 2019 updates, FamilyTreeDNA's Privacy Statement mentioned the term "law enforcement" only once—to reassure users that "[i]f compelled to disclose your Personal Information to law enforcement, we will do our best, unless prohibited by law, to provide you with notice." Id. § 5.D.

[356] See supra notes 311–315 and accompanying text (describing changes GEDmatch made to its site policy, user home page, and other practices within a month of learning that investigators had used GEDmatch in investigating the Golden State Killer case).

[357] See FamilyTreeDNA March 2019 Updates, supra note 31.

[358] Account Settings: Privacy & Sharing, FamilyTreeDNA, https://www.familytreedna.com/my/privacy-sharing (last visited Sept. 10, 2019) (locate "Law Enforcement Matching," under "Matching Preferences," under "Privacy & Sharing," under "Account Settings") (on file

Yet even now, privacy practices at FamilyTreeDNA leave much to be desired—and give rise, at best, to questionable consent to law enforcement access. For one thing, FamilyTreeDNA has made declining law enforcement access to one's genetic data difficult to accomplish. Under the March 2019 updates, existing U.S.-based FamilyTreeDNA users were preemptively opted in to law enforcement use of their genetic data.[359] New users, meanwhile, are not squarely presented with an option to decline such use. Rather, as part of joining the site, new users consent generally to "Participate in Matching," which encompasses "different matching levels, including Law Enforcement Matching."[360] For all users, opting out of Law Enforcement Matching requires the user to access their "Privacy & Sharing" settings and unclick "Opt in to Law Enforcement Matching."[361] Declining law enforcement matching is therefore more cumbersome, less obvious—and accordingly, more unwitting—for FamilyTreeDNA users than for any user at GEDmatch.

Moreover, FamilyTreeDNA still holds itself out as uniquely committed to user privacy, despite its expanding cooperation with law enforcement. To be sure, FamilyTreeDNA has taken steps to make its program of law enforcement cooperation more transparent. Most conspicuously, it has made law enforcement use of consumer genetic data the subject of an advertisement.[362] It has also revised its Terms of Service and Privacy Statement to delineate explicitly the scope of permitted law enforcement use.[363] And it has created a Law Enforcement Guide that describes the circumstances under which FamilyTreeDNA authorizes law enforcement

with the Virginia Law Review Association); see also Marcus, supra note 29 (reporting that "less than 2% of customers have requested opting out of law-enforcement searches").

[359] FamilyTreeDNA March 2019 Updates, supra note 31; see Ram & Roberts, supra note 3, at 707. Significantly, unlike U.S.-based users, existing E.U.-based users were preemptively opted out of law enforcement matching when FamilyTreeDNA introduced this option. See FamilyTreeDNA March 2019 Updates, supra note 31 ("User accounts created prior to March 12th, 2019 that are flagged as an EU account have been opted out of Law Enforcement Matching but may choose to opt in.").

[360] Consent to Participate in Matching, FamilyTreeDNA, https://www.familytreedna.com/-legal/consent/matching [https://perma.cc/QA3H-BKZW] (last visited August 18, 2019).

[361] See Account Settings: Privacy & Sharing, supra note 358.

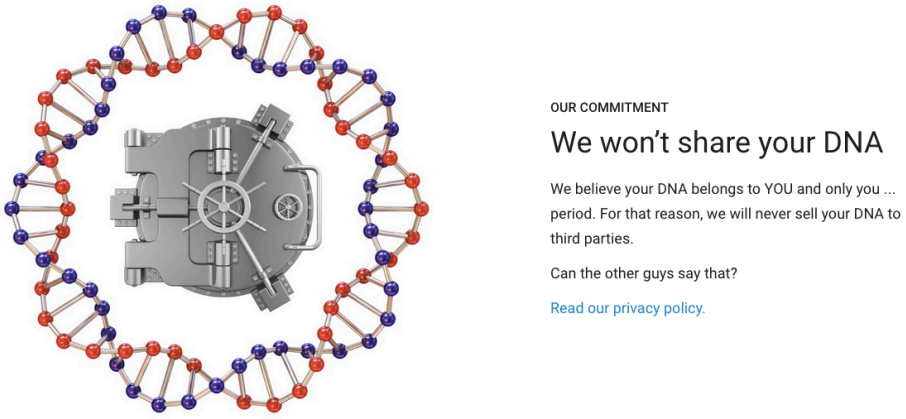
[362] See Zhang, supra note 33.

[363] Terms of Service, FamilyTreeDNA § 6.B.xii (Mar. 12, 2019) [hereinafter FamilyTreeDNA March 2019 Terms of Service], https://www.familytreedna.com/legal/terms-of-service [https://perma.cc/3UZ6-3YPF]; FamilyTreeDNA Privacy Statement, FamilyTreeDNA § 5.D (May 7, 2019) [hereinafter FamilyTreeDNA May 2019 Privacy Statement], https://www.familytreedna.com/legal/privacy-statement [https://perma.cc/EKY2-4TT7].

use of its database.[364] These changes make FamilyTreeDNA's policy regarding law enforcement access more transparent and understandable to ordinary users, and that is to FamilyTreeDNA's credit.

But these changes are often in tension with FamilyTreeDNA's more prominent statements about a commitment to user privacy, and they may be too little, too late. The policy revisions, for instance, are often buried deep in the relevant documents: the Terms of Service describe law enforcement access first in Section 6.B.xii,[365] while the Privacy Statement discusses such access first in Section 4.B.viii.[366] Meanwhile, unlike GEDmatch's notable and noticeable announcements on its user home page of its policy regarding law enforcement access, FamilyTreeDNA's homepage (as Figure 1 shows) continues to emphasize the platform's asserted commitment to user privacy.

Fig. 1. FamilyTreeDNA homepage summary of privacy policy[367]



[364] See FamilyTreeDNA Law Enforcement Guide, FamilyTreeDNA, https://www.familytreedna.com/legal/law-enforcement-guide [https://perma.cc/6M83-2E9Q] (last visited July 17, 2019).

[365] FamilyTreeDNA March 2019 Terms of Service, supra note 363.

[366] FamilyTreeDNA May 2019 Privacy Statement, supra note 363 ("FamilyTreeDNA uses your Genetic Information for the following primary purposes . . . [to c]omply with requests from law enforcement or their authorized representatives that meet our Law Enforcement Guidelines . . . .").

[367] FamilyTreeDNA, supra note 334.

In sum, FamilyTreeDNA initially said one thing, but did another—and even its revised practices continue to employ inconsistent and confusing representations of the platform's approach to user privacy and access. At best, FamilyTreeDNA facilitates the largely unwitting and often presumed consent of its users to law enforcement access. That ought not satisfy a post-*Carpenter* examination of consent to law enforcement access in the digital context.

CONCLUSION

Genetic data is highly sensitive and presumptively private. In a variety of circumstances, however, individuals make their genetic data available to third parties, including increasingly through genealogical or other consumer genetic services. In the past, such data sharing was likely sufficient, standing alone, to negate an individual's constitutionally protected expectation of privacy in her genetic data. The Supreme Court's recent decision in *Carpenter*, however, opens the way for more robust and nuanced assessments of what constitutes a reasonable expectation of privacy for data in third-party hands.

Genetic information is precisely the kind of data in which an individual ought to maintain an expectation of privacy after *Carpenter*—even when that data is shared with a third party. Genetic data is nearly always "deeply revealing," and the rapidly growing use of consumer and other genetic testing services will soon make third-party access to an individual's genetic data commonplace and nearly unavoidable. Courts should act now, in recognition "of more sophisticated systems that are already in use or in development,"[368] to protect the important Fourth Amendment interests implicated when the government seeks to access genetic data in third-party hands.

But that does not mean that all genetic data stored in third-party repositories is beyond government reach. Even where an individual harbors a reasonable expectation of privacy, she may nonetheless consent to its search by the government. Where, in view of genuine alternatives, an individual has knowingly and voluntarily agreed to permit the government to make use of her data for crime detection purposes, she has little basis to object when such use occurs. By the same token, however, an

[368] Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

individual ought to be able to rely on promises of protection against government access to her data.

As the dramatically divergent responses of genealogical genetic platforms to the arrest of the alleged Golden State Killer make clear, privacy policies and related practices can be highly visible and informative. Users of services like 23andMe, Ancestry, and to some extent even GEDmatch should take comfort in knowing where they—and their genetic privacy—stand with each of those services. These services have adopted different approaches to user privacy, but each has been clear about what that approach is. Meanwhile, other service providers, including FamilyTreeDNA, should take note.

Explicit, visible, and understandable privacy practices are well within reach. Users are entitled to clear information about whether and how their data will be shared or matched with others, including law enforcement. Conflicting statements and presumed consent undermine the possibility of genuine and robust consent. And in the absence of such consent, an expectation of privacy for deeply revealing information like genetic data should persist. The practices of genetic genealogy platforms provide a lens for reexamining the relationship between privacy practices, expectations of privacy, and consent—and they should be instructive across the diverse range of digital networks of which modern Americans are a part.