IP Theory

Volume 12 | Issue 2 Article 2

Spring 3-2023

A Hot Spit-Take: Why the Supreme Court Will Hold That There Is No Privacy Interest in Commercial DNA Data

Mounir Jamal
mojamal@iu.edu

A HOT SPIT-TAKE: WHY THE SUPREME COURT WILL HOLD THAT THERE IS NO PRIVACY INTEREST IN COMMERCIAL DNA DATA

Volume 12 | Issue 2 | Article 2

Mounir Jamal
2022-2023

A HOT SPIT-TAKE: WHY THE SUPREME COURT WILL HOLD THAT THERE IS NO PRIVACY INTEREST IN COMMERCIAL DNA DATA

Mounir Jamal

INTRODUCTION

Tracing one's family history can be incredibly enriching; however, thirty-four percent of Americans cannot trace their family tree past their grandparents.[1] As a result, Americans over the past decade have used commercial DNA networks like Ancestry.com, 23andMe, and CRI Genetics to learn more about their genetic past.[2] These companies use unique methods to analyze a consumer's DNA, but the essence of the process is the same across all companies. After a consumer sends in their DNA sample (typically through an at-home spit test kit), the DNA is amplified and organized by chromosome type.[3] Chromosome types include the paternal Y chromosome, the maternal X chromosome, and the twenty-two non-sex chromosomes that code for other features.[4] The code found in these chromosomes is then compared to reference data sets stored in the massive libraries at commercial DNA networks.[5] Through this meticulous comparison, these networks reveal the origins of a consumer's DNA and can flag other users in the system with similar genetic coding as potential distant relatives.

The prospect of meeting a long-lost relative or discovering ancestral origins makes the booming commercialization of this market of little to no surprise. However, what happens to this DNA data that is consistently augmenting the libraries of these commercial DNA networks? More specifically, do individuals have a privacy interest in their DNA after it has

---

[1] Nicola Haslam, *A Third of Americans Can't Name All of Their Grandparents, Study Finds*, SWNS DIGITAL (Dec. 19, 2018), https://www.swnsdigital.com/2018/12/a-third-of-americans-cant-name-all-of-their-grandparents-study-finds/#:~:text=A%20third%20of%20Americans%20are,it%20comes%20to%20their%20heritage.

[2] *See* Antonio Regalado, *More Than 26 Million People Have Taken an At-Home Ancestry Test*, MIT TECH. REV. (Feb. 11, 2019), https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/; *see also Three Mistakes to Avoid When Shopping for a DNA Test: Your Free Guide to the Best Valued DNA Tests*, GENETICS DIGEST (2020), https://geneticsdigest.com/best_ancestry_genealogy_dna_test/index.html?gclid=EAIaIQobChMI55yV4cie7AIVRNbACh3VyAOxEAAYAiAAEgLfmvD_BwE (ranking the top three DNA testing companies to use and placing CRI at number one).

[3] Rafi Letzter, *How Do DNA Ancestry Tests Really Work?*, LIVESCIENCE (June 4, 2018), https://www.livescience.com/62690-how-dna-ancestry-23andme-tests-work.html.

[4] *Id.*

[5] *Id.*

been submitted to these networks, and if so, should there be any exceptions to this rule?

In *Carpenter v. United States*, a divided Supreme Court held that an individual maintains a legitimate expectation of privacy, for Fourth Amendment purposes, in the record of his or her physical movements as captured through cell-site location information.[6] As a result of *Carpenter*, numerous scholars have published work predicting the implications of the case on other technologies such as commercial DNA data.[7] This Article will not add to the abundance of scholarly work concluding that, based on *Carpenter*, a privacy right exists in DNA data. Instead, this Article will argue the opposite, with a twist. This Article argues that a privacy right does not exist in DNA data voluntarily submitted to commercial DNA networks based on the test promulgated in *Carpenter*; however, this Article argues alternatively that even if the Supreme Court holds a privacy interest in DNA data held in commercial DNA network databases (or if states choose to statutorily protect this interest), there should be an exception for parties that use the data for clinical research and that meet a good-faith standard.

Part I of this Article gives an overview of DNA data and how it is used while providing legal context on DNA data law and regulation. Part II focuses on the *Carpenter* decision and its descendants. Part III will apply the majority's holding to commercial DNA databases. The final section in Part III will discuss an argument in the alternative: a pharmaceutical exception to commercial DNA data privacy for parties conducting medical research and meeting a good-faith standard.

I. OVERVIEW OF DNA DATA: USES AND THE CURRENT LAW

For those unfamiliar, deoxyribonucleic acid (DNA) is the double-helix molecule that codes for the genetic makeup of all living things.[8] DNA consists of nucleotides (Adenine, Thymine, Guanine, and Cytosine) that code for the proteins that ultimately yield our unique characteristics (e.g. hair

[6] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
[7] *See, e.g.*, Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357 (2019); Drew M. Baldwin, *Redefining the Third-Party Doctrine:* Carpenter*'s Effect on DNA Privacy*, 108 KY. L.J. 153 (2020).
[8] *DNA*, WHAT IS BIOTECHNOLOGY?, https://www.whatisbiotechnology.org/index.php/science/summary/dna/#:~:text=Definition,and%20functioning%20of%20the%20body (last visited June, 28, 2021).

color, eye color, etc.) and serve as the building blocks for our biological development (e.g. physical growth, immune capabilities, etc.).[9] The genetic code for a single individual is a string of more than six billion of these nucleotides,[10] and it is this very string, or significant portions of it, that is stored in commercial DNA databases as DNA profiles of the consumers.

A. Practical Uses of DNA Data in the Public and Private Sectors

DNA data can be used in a variety of ways. For instance, DNA data is used extensively for research and discovery, even being used in the late twentieth century and early twenty-first century to try and answer the question, "who and what are we?"[11] The following sections focus on two particular uses relevant to DNA data and privacy: (1) the use of commercial DNA data to identify potential suspects in cold cases and (2) the use of DNA in clinical and medical research.

1. Law Enforcement

Forensic evidence has long been used to help solve criminal cases. Examples of this include ballistics reports, fingerprint tracings, and most importantly, DNA evidence.[12] DNA evidence found at a crime scene is cross-referenced with records in DNA databases in order to identify potential

[9] *Genetic Code*, SCIENCEDAILY (2020), https://www.sciencedaily.com/terms/genetic_code.htm; *see also* Eugene V. Koonin & Artem S. Novozhilov, *Origin and Evolution of the Genetic Code: The Universal Enigma*, IUBMB LIFE (Feb. 2009), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3293468/ (explaining how sequences of three DNA nucleotides, following translation by RNA, lead to the production of various amino acids that will ultimately make up proteins).

[10] *Size Matters: A Whole Genome Is 6.4B Letters*, VERITAS GENETICS (July 28, 2017), https://www.veritasgenetics.com/our-thinking/whole-story/#:~:text=A%20Real%20Human%20Genome%20is,pairs)%20Long%20%E2%80%94%20Not%203.2%20Billion.

[11] *See, e.g.*, *The Human Genome Project*, NAT'L HUM. GENOME RES. INST. (2020), https://www.genome.gov/human-genome-project (describing "one of the great feats of exploration in history" when an international team of researchers mapped out the complete genetic sequence of the human being).

[12] Dawn Lomer, *15 Types of Evidence and How to Use Them*, I-SIGHT (Apr. 6, 2016), https://i-sight.com/#:~:text=Forensic%20Evidence,a%20person%27s%20guilt%20or%20innocence.

suspects.[13] In the 1980s, the federal government initialized a system called the Combined DNA Index System (CODIS) that expedited the shared exchange of DNA profiles between state and local law enforcement across the country.[14] However, this system is constrained by the fact that the DNA profiles available are of those obtained from convicted offenders.[15] Consequently, trying to match DNA evidence found at a crime scene of a crime committed by a first-time offender is essentially impossible. This is where the complex potential of commercial DNA networks becomes clear.

Since commercial DNA networks contain the DNA profiles of millions of individuals, most of whom are not previous criminal offenders, these networks offer the possibility of matching forensic DNA to first-time offenders. Law enforcement has already successfully used commercial DNA networks for this very benefit.

In April of 2018, the notorious "Golden State Killer" was arrested.[16] The Golden State Killer was a notorious serial killer between 1960 and 1980.[17] He committed over a dozen murders and over fifty rapes throughout California, with all of these crimes remaining unsolved until law enforcement sought the use of the commercial DNA network, GEDMatch.[18] Law enforcement had maintained a frozen sample of DNA found at the crime scenes of multiple murders. This DNA sample was submitted to the GEDMatch database, which then yielded results linking the DNA to distant relatives in the network.[19] From there, law enforcement traced the information back to Joseph DeAngelo, the individual now sitting behind bars, guilty of the horrific crimes of the Golden State Killer.[20] Though the Golden State Killer case is likely the most famous solved cold case arising out of the

---

[13] *Advancing Justice Through DNA Technology: Using DNA to Solve Crimes*, U.S. DEP'T JUST. (Mar. 7, 2017), https://www.justice.gov/archives/ag/advancing-justice-through-dna-technology-using-dna-solve-crimes.
[14] *Id.*
[15] *See id.*
[16] Jocelyn Kaiser, *We Will Find You: DNA Search Used to Nab Golden State Killer Can Home in on About 60% of White Americans*, SCI. MAG. (Oct. 11, 2018, 2:00 PM), https://www.sciencemag.org/news/2018/10/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white.
[17] Drew M. Baldwin, *Redefining the Third-Party Doctrine:* Carpenter*'s Effect on DNA Privacy*, 108 KY. L.J. 153, 167 (2020).
[18] *Id.*
[19] *Id.*
[20] Eliott C. McLaughlin & Stella Chan, *Hearing Details Ghastly Crimes of Golden State Killer as He Pleads Guilty to Killings*, CNN (June 29, 2020, 9:13 PM), https://www.cnn.com/2020/06/29/us/golden-state-killer-plea-expected/index.html.

use of commercial DNA networks, many other cold cases have likewise been cracked.[21]

This Article, unlike most scholarly pieces on this topic, is not focused on the law enforcement uses of commercial DNA networks. However, the sheer abundance of examples in this field requires a brief summary of the associated privacy concerns. One common concern is the issue of familial informants. By uploading DNA to a commercial network, law enforcement could use one's data against members of his or her family; the reciprocal case could be true as well, where a family member's submission could then be used against an individual who never interacted with these commercial DNA networks.[22] Such a case may seem far-fetched or unlikely, but Sonia Suter of George Washington University put it best: "'There is a tendency . . . to minimize the privacy costs [of a technology] because the gains are so great.'"[23] In other words, people tend to disregard the privacy concerns associated with a technology like DNA profiling because tangible benefits (like the solving of horrific cold cases), at least from a distance, outweigh these concerns. As a society, we must decide where our balance falls. Are individuals willing to tolerate such privacy concerns if it means unraveling decades-long cold cases? While this is a difficult question to answer regarding the intricate benefits of law enforcement, the benefits of pharmaceutical and clinical research outweigh the privacy concerns associated with commercial DNA networks.[24]

2. Pharmaceutical and Medical Research

Critics often overlook the vast benefits of pharmaceutical and clinical research via commercial DNA networks. If the law develops a privacy interest in DNA submitted to these networks, the doctrine should include an exception for pharmaceutical and biomedical companies meeting a good-faith standard.

At this point in our political discourse, it is almost cliché to complain about the expenses of pharmaceutical drugs and to admonish pharmaceutical companies for their "greed." However, *why* are these drugs so expensive?

---

[21] Kaiser, *supra* note 16; *see also* Baldwin, *supra* note 17, at 168 (describing the process behind solving the "Grim Sleeper" cold case).

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

[23] *Id.*

[24] *See infra* Part I.A.2.

The answer lies in the exorbitant cost of production as well as the high failure rate associated with drugs reaching clinical trials. Taking a new drug to market costs pharmaceutical companies about $2.6 billion; further, the rate of success of drugs that make it through clinical trials is only about twelve percent.[25] This dreadful failure rate is a major hurdle for pharmaceutical companies to traverse. As Joseph DiMasi, Director of Economic Analysis at Tufts University, explained, "Approximately seven out of eight compounds that enter the clinical testing pipeline will fail in development."[26] Reducing these costs and risks of failure can lower the overhead on drug production and consequently lower the cost on the consumer.[27]

One way that commercial DNA data can cut at these thorns of pharmaceutical development is through streamlined research. For hundreds of years, medicine has focused on treating the *symptoms* of different diseases, but recently, new methodologies focus on treating the *source*: DNA.[28] For example, because a majority of commercial DNA network customers choose to answer questionnaires on their health, pharmaceutical companies can amass huge collections of data that can "provide[] clues on the interplay between genetics and particular ailments, creating potentially fruitful avenues for drug discovery."[29] Correlations between certain disease-coding genes, individuals who show no symptoms, and surrounding gene traits can streamline research and target particular gene strands for drug discovery.[30] Through the same underlying principles, pharmaceutical companies can also create drugs that "edit" or "silence" genes found to be linked to certain diseases.[31] Research even indicates that rather than using linear strands, DNA

---

[25] Thomas Sullivan, *A Tough Road: Cost to Develop One New Drug Is $2.6 Billion; Approval Rate for Drugs Entering Clinical Development is Less Than 12%*, POL'Y & MED. (Mar. 21, 2019), https://www.policymed.com/2014/12/a-tough-road-cost-to-develop-one-new-drug-is-26-billion-approval-rate-for-drugs-entering-clinical-de.html#:~:text=Developing%20a%20new%20prescription%20medicine,the%20Journal%20of%20Health%20Economics.

[26] *Id.*; *see also* Patricio Ledesma, *How Much Does a Clinical Trial Cost?*, SOFPROMED (Jan. 2, 2020), https://www.sofpromed.com/how-much-does-a-clinical-trial-cost/ ("The average cost of phase 1, 2, and 3 clinical trials across therapeutic areas is around $4, 13, and 20 million respectively.").

[27] *See* Sullivan, *supra* note 25.

[28] Josh Fischman, *The DNA Drug Revolution*, SCI. AM. (Jan. 1, 2020), https://www.scientificamerican.com/article/the-dna-drug-revolution/.

[29] Denise Roland, *How Drug Companies Are Using Your DNA to Make New Medicine*, WALL ST. J. (July 22, 2019), https://www.wsj.com/articles/23andme-glaxo-mine-dna-data-in-hunt-for-new-drugs-11563879881?mg=prod/com-wsj.

[30] *See id.*

[31] Fischman, *supra* note 28.

spheres have an enhanced ability to enter cells and perform these editing processes, which can potentially reduce the failure rate discussed previously.[32] Focusing on the source of diseases, the DNA code itself, can lead to streamlined research and unique drug processes that can lower the cost of development.[33]

Another practical use of DNA data from commercial networks would be the dramatic increase in efficiency of generating clinical trials. Having an entire database of DNA profiles at one's disposal that can be filtered for certain genes, traits, and ailments can result in instant organization and creation of specific clinical trial groups needed for particular drugs. For example, pharmaceutical giant, Glaxo, entered into an agreement with 23andMe in order to "accelerate the costly and arduous process of finding patients to join clinical trials."[34] This agreement has already begun to yield early results that demonstrate the benefits of commercial DNA networks in this context. One of the drugs Glaxo is currently pursuing targets a rare mutation in a gene called LRRK2 that increases the risk of Parkinson's Disease.[35] Only 0.1% of the population carries this mutation, so it becomes almost impossible to find carriers using traditional clinical trial recruitment tactics (such as advertisements).[36] On the other hand, 23andMe's data has contact details for 7500 carriers, carriers that would otherwise likely not have been discovered.[37] Dr. John Lepore, a lead researcher at Glaxo, estimates that this modernization of clinical trial recruitment could shave "months, if not years" off of the process.[38]

Different factors influence the cost of a clinical trial. These include the size of the study, the location, and the number of clinical sites needed to service the entire clinical trial group.[39] Having access to commercial DNA data can significantly cut at these factors.[40] Further, commercial DNA

---

[32] *Id.*

[33] Despite being a relatively new field of research and pharmaceutical focus, there are already fourteen approved DNA-related drugs on the market, suggesting the promise and utility of research and development tied to this area. *Id.*

[34] Roland, *supra* note 29.

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *Id.*

[39] Ledesma, *supra* note 26.

[40] For example, the size of a study will no longer be as influential of a factor because even clinical trials requiring exceptionally large sample sizes can be put together quickly by filtering DNA profiles in commercial networks. *See id.*

networks can streamline research on genetic illnesses and help perpetuate the development of DNA-related drugs. All of these potential benefits and efficiency improvements can lower the cost of production, which can then lower the cost of drugs to the consumer.

B. Current Legal Context

The following sections will serve to provide context surrounding the law as it stands with DNA data privacy as well as the current state of the Supreme Court of the United States and its impending judicial philosophies.

1. Federal Law

The federal government has been rather reserved in regulating DNA data and commercial DNA networks. In 2010, the Food and Drug Administration (FDA) sent warning letters to 23andMe regarding the practices involved with some of their genetic tests, resulting in the company briefly terminating the sale of health-related genetic tests.[41] By 2015, the FDA had started to approve health-related genetic tests from commercial DNA networks, including those for breast cancer gene mutations, Bloom Syndrome, and more.[42]

In reality, the Federal Trade Commission (FTC) has really been the only regulating power on the federal side attempting to keep commercial DNA networks in check. A notable example of the FTC's regulatory power was a complaint filed against GeneLink, Inc. in May of 2014.[43] GeneLink used consumer genetic tests to match customers with nutritional supplements and skincare products.[44] The FTC alleged that the company's practices were unfair and deceptive because they "[f]ailed to implement reasonable policies and procedures to protect the security of consumers' personal information."[45] To resolve the dispute, GeneLink entered into a consent agreement with the FTC requiring them to submit to audits and maintain security data records.[46]

---

[41] Samuel A. Garner & Jiyeon Kim, *The Privacy Risks of Direct-to-Consumer Genetic Testing: A Case Study of 23andMe and Ancestry*, 96 WASH. U. L. REV. 1219, 1228–29 (2019).
[42] *See id.* at 1229.
[43] *Id.* at 1230.
[44] *Id.*
[45] *Id.*
[46] *Id.*

Aside from administrative regulatory actions such as this, however, the federal government has yet to enact laws regarding DNA data privacy.

2. State Law

States have been more aggressive in regulating privacy related to commercial DNA networks.[47] In particular, states have focused their legislative agendas on genetic privacy issues. California is a prime example of this effort.[48] First, California's Genetic Information Nondiscrimination Act "extends the areas of protection from genetic discrimination to emergency medical services, housing, mortgage lending, education, and state funded programs."[49] California took a further step when it enacted the California Consumer Privacy Act of 2018 by categorizing genetic information as "personal information."[50]

This classification is significant for a few reasons. First, it represents an example of law that defines genetic privacy as "personal." This does not explicitly classify genetic data as an individual *right of privacy*; however, the California legislature seems to imply this leap. Second, the act, as written, currently contains no exception for pharmaceutical companies acting in good faith (as no state statute does).[51] This leaves room, as this Article argues, for such an exception to be written into the statute.[52]

3. The Future of the Supreme Court

With the appointment of Justice Amy Coney Barrett,[53] the Supreme Court is now comprised of six conservative Justices and three liberal Justices.[54] This conservative swing may prove to be consequential for future

---

[47] *Id.* at 1231 (stating that "thirteen . . . states effectively prohibit [commercial DNA network genetic tests], and twelve states limit access to [these tests] in certain aspects").
[48] *Id.* at 1232.
[49] *Id.* (citing Cal. Civ. Code § 51 (West 2011)).
[50] Cal. Civ. Code § 1798.140(o) (West 2020).
[51] *See generally id.*
[52] *See infra* Part III.B.
[53] Nicholas Fandos, *Senate Confirms Barrett, Delivering for Trump and Reshaping the Court*, N.Y. TIMES (Oct. 26, 2020), https://www.nytimes.com/2020/10/26/us/politics/senate-confirms-barrett.html.
[54] *The Political Leanings of the Supreme Court Justices*, AXIOS (June 1, 2019), https://www.axios.com/supreme-court-justices-ideology-52ed3cad-fcff-4467-a336-8bec2e6e36d4.html (depicting the Justices along a graph of ideology, with Justices Thomas, Kavanaugh, Gorsuch, Alito, and Chief Justice Roberts as conservative, and Justices Breyer, Kagan, Sotomayor, and the late Justice Ginsburg as liberal).

applications of *Carpenter*. In *Carpenter,* four traditionally conservative Justices dissented (Justices Kennedy, Thomas, Gorsuch, and Alito).[55] Chief Justice Roberts was the lone defector from the conservative side, a rather commonplace phenomenon in recent years.[56] In predicting the implications of *Carpenter*,[57] it will be imperative to understand the judicial and philosophical direction of the Court, specifically, Justice Barrett's views on data privacy.

In *United States v. Wanjiku*, then-Judge Barrett declined to extend *Carpenter* in a decision concerning a warrantless search of a criminal defendant's cell phone, concluding that law enforcement had justifiably relied on precedent that required nothing more than reasonable suspicion in order to conduct a warrantless search at the U.S. border.[58] Further, in *Gadelhak v. AT&T Services*, Judge Barrett ruled against consumer privacy concerning automatic telephone dialing systems used by corporations.[59] These decisions by themselves do not necessarily mean that Justice Barrett would overrule the recent precedent of *Carpenter*; however, Justice Barrett's track record seems to suggest that she will at least attempt to find no privacy rights in other technologies.[60] Will this conservative ideology of the new Justice combined with a now-supermajority be enough for the Court to hold no privacy right in commercial DNA? As Barrett stated in her confirmation hearing, "The Constitution . . . [is] written at a level of generality that's specific enough to protect rights, but general enough to be lasting."[61] Based on this philosophy, a strong conservative majority on the Court could, in theory, apply *Carpenter* differently to different technologies that are not specifically delineated in the Constitution: for example, commercial DNA data.

[55] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).
[56] *See, e.g.*, NFIB v. Sebelius, 567 U.S. 519 (2012) (Chief Justice Roberts joining liberal Justices to uphold the Affordable Care Act).
[57] *See infra* Part III.A.
[58] *Amy Coney Barrett and Privacy*, ELECTRONIC PRIVACY INFO. CTR. (2020), https://epic.org/privacy/barrett/.
[59] *Id.*
[60] *See id.*
[61] *Id.*

II. *CARPENTER* AND ITS DESCENDANTS

Carpenter v. United States has been discussed and analyzed thoroughly in a multitude of law review articles on an assortment of topics.[62] These scholarship pieces argue that individuals have a privacy interest in DNA submitted to commercial DNA networks. This Article argues the opposite. Thus, a review of the majority opinion is provided in this part of the Article. The factors of the *Carpenter* test are dissected in order to apply them in Part III. Thereafter, an example of *Carpenter* being applied to a recent case is presented.

A. Carpenter*'s Holding*

In *Carpenter*, the issue before the Court was "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements."[63] The facts of the case involve petitioner, Timothy Carpenter, who was charged with six counts of robbery after the Government seized cell-site records from MetroPCS that placed Carpenter's cell phone location at the scenes of the crimes and at the time the crimes were committed.[64] At the core of the case are individual rights under the Fourth Amendment, specifically, the privacy safeguards it offers individuals.[65] The Court denoted that "'the Fourth Amendment protects people, not places,' and . . . protect[s] certain expectations of privacy as well."[66]

The Court next discussed the third-party doctrine, the roots of which can be found in *United States v. Miller*.[67] In summation, the third-party doctrine provides that a person has no legitimate expectation of privacy in information that he or she voluntarily turns over to third parties;

---

[62] *See, e.g.*, Camille Mennen, *Reconciling Fourth Amendment Protection Standards with Modern Technology*, 14 TENN. J.L. & POL'Y 11 (2019) (providing a brief synopsis of the case and its application); Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205 (2018) (describing *Carpenter*'s place in the history of government regulation of surveillance).
[63] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).
[64] *Id.* at 2212–13.
[65] *See id.* at 2213.
[66] *Id.* (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).
[67] *Id.* at 2216 (citing United States v. Miller, 425 U.S. 435, 443 (1976)).

consequently, the Government is normally allowed to obtain such information without triggering Fourth Amendment protections.[68]

In its holding, the Court declined to extend the third-party doctrine to Carpenter's case "to cover these novel circumstances."[69] Instead, the Court laid out a test for determining whether a novel category of information or technology is protected under Fourth Amendment individual privacy.[70] While not explicitly defined, Chief Justice Roberts' conclusion in the majority opinion suggests that the Court promulgated three factors that must be considered: "(1) 'the deeply revealing nature' of the information [or technology]; (2) 'its depth, breadth, and comprehensive reach'; and (3) 'the inescapable and automatic nature of its collection.'"[71]

Chief Justice Roberts emphasized that the decision "[was] a narrow one" and did not "express a view on matters not before [the Court]."[72] In doing so, the Chief Justice made clear that the *Carpenter* doctrine leaves room for ample interpretation for other types of technologies; commercial DNA data would presumably fall under this umbrella.

B. The Carpenter *Factors*

1. "Deeply Revealing" Information

The first factor in the *Carpenter* test requires courts to consider whether a technology reveals information that is deeply revealing. This factor focuses on the intrinsic nature of the information; in other words, what does it actually convey to someone who has access to said information?[73]

The Court in *Carpenter* describes deeply revealing information as information that can express an individual's "familial, political, professional, religious, and sexual associations."[74] Recall that this case involved cell-site location data. Under these guidelines, this type of data clearly meets the

[68] *Id.*
[69] *Id.* at 2217
[70] *Id.* at 2217–20; *see also* Ohm, *supra* note 7, at 370 ("There is likely to be disagreement about the precise list of *Carpenter* factors, given the wide-ranging nature of the opinion.").
[71] Ohm, *supra* note 7, at 370 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018)).
[72] *Carpenter*, 138 S. Ct. at 2220.
[73] *Id.* at 2223.
[74] *Id.* at 2217 (citation omitted).

standards of the first factor of the test. Consider, for instance, an individual's visits to a church, mosque, synagogue, or other religiously affiliated institution. Someone with access to the individual's cell-site data could easily discover these visits and determine the individual's religious beliefs. This information precisely would be of the "deeply revealing" nature that the Court discusses. Similar examples would not be difficult to conjure for the other types of associations listed. However, what about information that does not relate to "familial, political, professional, religious, and sexual" relationships?

Deeply revealing information has additionally been construed to mean information that is either (1) sensitive or (2) intimate.[75] Sensitive information is defined as "information that can be used to cause an individual or group harm" while intimate information "reveals something important and not widely known about a relationship between individuals."[76] Again, one can see the application of these definitions in the context of *Carpenter*. One's location, derived from cell-site data, could, for example, reveal an individual's extramarital affair (e.g. location at the address of a mistress) or leave an individual susceptible to discrimination based on political beliefs (e.g. location data showing the individual at particular political conventions). This information would both be sensitive because it could harm the individual's reputation, job opportunities and more, and it is intimate because of its volatile consequences on personal and professional relationships.

In conclusion, the first factor of the *Carpenter* test requires courts to analyze the information of the technology intrinsically and determine whether it has the potential to convey deeply revealing information.

2. Depth, Breadth, and Comprehensive Reach

The second factor of the *Carpenter* test asks courts to protect information that has "depth, breadth, and comprehensive reach."[77] Similar to the first factor, this analysis asks courts to consider the information revealed by a technology *intrinsically*. Note that this factor truly has three subfactors that can be analyzed independently of one another: (1) depth, (2) breadth, and (3) comprehensiveness.

[75] *See* Ohm, *supra* note 7, at 371.
[76] *Id.*
[77] *Carpenter*, 138 S. Ct. at 2223.

The first subfactor, depth, really means the *quality* of the data that is stored.[78] After all, the data could not be "deeply revealing" if it lacked detail or precision. Within the *Carpenter* facts, this subfactor was met because the cell-site data could pinpoint an individual's location, as well as the time that the individual was there.[79]

The second subfactor, breadth, refers to a temporal component of information.[80] Specifically, courts analyze "how frequently the data is collected, and for how long the data has been recorded."[81] Cell-site data fulfills both of these temporal components. First, cell-site data is collected multiple times daily and is "continually logged for all of the 400 million devices in the United States."[82] Second, the Court found that cell-site data is held for up to five years; this was deemed a long enough recording period.[83]

The final subfactor, comprehensiveness, is relatively straight forward, referring to how many individuals can be accessed through a particular database.[84] In *Carpenter*, the cell-site database, in theory, had access to the 400 million devices used in the United States.[85] Though the Court does not delineate a particular quantity for this portion of the test, it clearly must be a substantial figure.

3. The Inescapable and Automatic Nature of Collection

The third and final factor of the *Carpenter* test is the information's "inescapable and automatic nature of collection."[86] The core of this factor is whether targeted individuals "may have assumed the risk of the data collection or knowingly exposed their information to the private party."[87] This factor has two subfactors: (1) inescapable information collection and (2) automatic information collection.

---

[78] *See* Ohm, *supra* note 7, at 372.
[79] *Carpenter*, 138 S. Ct. at 2220. *But see id.* at 2226 (Kennedy, J., dissenting) (implying imprecision on the part of cell-site data because the location could be within "a dozen to several hundred city blocks" of the crime scene).
[80] Ohm, *supra* note 7, at 372.
[81] *Id.*
[82] *Carpenter*, 138 S. Ct. at 2218.
[83] *Id.*
[84] Ohm, *supra* note 7, at 373.
[85] *Carpenter*, 138 S. Ct. at 2218.
[86] *Id.* at 2223.
[87] Ohm, *supra* note 7, at 376.

In *Carpenter*, the cell-site data was considered "inescapable" because it related to a device (the cell phone) that is essentially a requirement to function in society.[88] In other words, because individuals *must* be attached at the hip to their phones, and because by their nature these phones continually collect location data at cell-sites, the collection is inescapable. On the other hand, automatic collection describes information collection that offers little awareness to the individual and provides "no meaningful opportunity to opt out."[89] With cell-site data's continual collection, cell phone users are offered no opportunity to opt-out of having their location detected every time they utilize their cell network; further, most users do not even realize that this data is being collected.[90]

In conclusion, the Court found that the information collected through cell-site data met all of the factors described above, and as a result, such information merited Fourth Amendment privacy protection.

C. Recent Applications of Carpenter

Have lower courts chosen to extend *Carpenter*'s doctrine to other technologies since the opinion was published in 2018? A scan of *Carpenter* descendants suggests that the answer to this question is no.[91] There are many cases that have limited *Carpenter*'s scope.[92] Two in particular illustrate this point.

In *United States v. Moore-Bush*, the First Circuit declined to extend *Carpenter* to data consisting of images taken by pole cameras.[93] The court in particular focuses on precision and comprehensiveness of pole camera data, noting that these cameras do not "monitor and catalogue every single

[88] *Id.* at 376–77.
[89] *Id.* at 377.
[90] *See* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.
[91] *See* Nathaniel Sobel, *Four Months Later, How Are Courts Interpreting* Carpenter*?*, LAWFARE BLOG (Oct. 18, 2018, 8:57 AM), https://www.lawfareblog.com/four-months-later-how-are-courts-interpreting-carpenter (discussing hesitation to extend *Carpenter* to other technologies and citing the Fifth Circuit's restriction of *Carpenter* to data that reveals a "person's day-to-day movement").
[92] *Id.*
[93] 963 F.3d 29, 43 (1st Cir. 2020).

movement" of an individual, nor do they "generate a precise . . . record of a person's public movements."[94] In *United States v. Gayden*, the Eleventh Circuit likewise declined to extend *Carpenter* to patient prescription records held by third parties.[95] There, the court focused on the "intimacy" of the data and found that *Carpenter* did not apply to Gayden's case because prescription drug data does not provide "an intimate window into a person's life" like the cell-site data at issue in *Carpenter*.[96]

The federal appellate courts have, for the most part, chosen to limit *Carpenter*'s scope and test. This should inform practitioners that, at least until another burgeoning, data-collecting technology reaches the eyes of the Supreme Court of the United States, lower courts will tend to hold that an individual has no right to privacy in such data collected by third parties.

III. *CARPENTER*'S FUTURE WITH DNA COMMERCIAL DATA

Most scholars believe that DNA data submitted to commercial networks like 23andMe and Ancestry.com falls within the *Carpenter* test as information protected by the right to privacy.[97] Based on the *Carpenter* factors discussed previously,[98] the trend of courts to avoid extending *Carpenter* to other technologies,[99] and the expansions of the conservative majority in the Supreme Court,[100] the Court is unlikely to hold that an individual privacy interest exists in commercial DNA data. Further, even if the Court holds that a privacy interest exists (or if laws are enacted protecting this interest), the use of the data for medical research under a good-faith standard should be excused.

---

[94] *Id.* at 45.
[95] 977 F.3d 1146, 1151 (11th Cir. 2020).
[96] *Id.* at 1152 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)).
[97] This portion of the Article will argue against some points made by Natalie Ram and Drew Baldwin in favor of finding a privacy right in commercial DNA data. *See* Baldwin, *supra* note 7, at 170 (arguing that commercial DNA data is protected because it is not truly voluntary); *see also* Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1380 (2019) (arguing for an individual's right to privacy in genetic data).
[98] *See supra* Part II.B.
[99] *See supra* Part II.C.
[100] *See supra* Part I.B.3.

A. Predicting Commercial DNA Data's Place After Carpenter

While improving individuals' rights to privacy is something most logical citizens would support, it is optimistic to believe that protections under *Carpenter* will be extended to commercial DNA data based on the test's factors, recent judicial applications, and the future of the Court itself.

1. DNA May Be "Deeply Revealing," But Is This Enough?

The first factor of the *Carpenter* test asks whether the information or technology is "deeply revealing." As discussed,[101] the test looks to expressions of an individual's "familial, political, professional, religious, and sexual associations" as a way to see if this prong is met. Does commercial DNA (and for purposes of this factor, really just DNA generally) fit into this prong? Possibly. DNA can obviously reveal familial associations between individuals; after all, discovering these relationships is one of the major reasons that consumers participate in these networks.[102] DNA can even potentially reveal an individual's sexual orientation, which adds to its deeply revealing nature with respect to "sexual associations."[103] Thus, even though DNA on its own cannot reveal an individual's religious, political, or professional associations, it seems to convey enough information from the other categories to suffice under this prong of the test.

Note, the first factor has also been construed to mean either sensitive or intimate data.[104] DNA data likewise fulfills these definitions of deeply revealing information. One commonly cited example of harm that can be caused by DNA data information is discrimination, particularly in the workplace.[105] For example, DNA data can describe innate disorders or ailments (e.g. dyslexia or ADHD) that an employer, unfairly, finds undesirable in an employee. In doing so, an employer could consciously (or subconsciously) decide not to hire a particular candidate based on these factors. This is just one example of the potential harm that DNA data can cause due to the sensitive and intimate information it reveals.

---

[101] *See supra* text accompanying note 74.
[102] *See* Letzter, *supra* note 3.
[103] Jocelyn Kaiser, *Genetics May Explain up to 25% of Same-Sex Behavior, Giant Analysis Reveals*, SCI. MAG. (Aug. 29, 2019, 2:00 PM), https://www.sciencemag.org/news/2019/08/genetics-may-explain-25-same-sex-behavior-giant-analysis-reveals.
[104] *See supra* text accompanying note 75.
[105] *See* Ram, *supra* note 97, at 1383.

The caveat, however, is the ease with which this information could actually be deeply revealing. Recall, the data must be analyzed *intrinsically* under this factor of the test.[106] How easy is it to actually retrieve this information from commercial DNA data? As one scholar suggests, DNA data is "at least as sensitive as [cell-site] location data."[107] But is it really? The cell-site data in *Carpenter* revealed specific data points that provided actual locations of the cell phone users.[108] An individual with little skill in cell data could access a cell phone user's location simply by looking at the dataset. On the other hand, commercial DNA data is not as easy to analyze. For one, commercial DNA data is anonymized.[109] Second, the data consists of strings of nucleotides comprising genes.[110] While it is possible to "deanonymize" this data, the level of expertise needed to actually sift through the data, translate the information to something that could harm the individual, and then actually identify the individual requires the expertise of someone with the skill level of a computational biologist.[111]

Carpenter did not focus on the ease with which information from cell-site data could be "deeply revealing." However, despite having the *potential* to be as "deeply revealing" as cell-site data, commercial DNA data is distinguishable in its difficulty to translate and the heightened skill required to deanonymize it. This makes commercial DNA data's fulfillment of the first *Carpenter* factor, though likely, at least questionable.

2. Commercial DNA Likely Fulfills the Depth, Breadth, and Comprehensive Reach Factor

The second *Carpenter* factor asks whether the information has "depth, breadth, and comprehensive reach." Of the three overarching factors in the *Carpenter* test, this factor is the easiest for commercial DNA data to fulfill, though even this factor may present some obstacles. Commercial DNA data, like with the first factor, must be considered intrinsically in this analysis.

---

[106] *See supra* text accompanying note 75.
[107] Ram, *supra* note 97, at 1387.
[108] Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).
[109] *See* Baldwin, *supra* note 7, at 170.
[110] Sang Yup Lee, *DNA Data Storage Is Closer Than You Think*, SCI. AM. (July 1, 2019), https://www.scientificamerican.com/article/dna-data-storage-is-closer-than-you-think/.
[111] *See* Megan Molteni, *Genome Hackers Show No One's DNA Is Anonymous Anymore*, WIRED (Oct. 11, 2018, 2:04 PM), https://www.wired.com/story/genome-hackers-show-no-ones-dna-is-anonymous-anymore/.

Regarding "depth," commercial DNA data likely passes muster due to its detail and precision.[112] Commercial DNA data is about as detailed as data can get, describing an individual consumer's DNA down to the nucleotide.[113] Additionally, regarding bigger picture familial associations, commercial DNA data tends to be "very good at determining close family relations such as siblings or parents."[114] On the other hand, as one expands beyond family relations into other information that DNA can reveal, this precision decreases. For example, forty percent of DNA variants associated with specific diseases from commercial DNA databases were shown to be false positives when the raw data was reanalyzed.[115] Is it enough that commercial DNA data is precise for only some categories (like close familial associations) and not others? *Carpenter*'s majority seemed to consider cell-site data's precision to suffice despite strong disagreement from the conservative dissent.[116] A more conservative Supreme Court may choose to side with Justice Kennedy's dissent on this issue with respect to commercial DNA data.

Regarding "breadth," commercial DNA data is once again ambiguous. First, the *frequency* of data collection is quite low, cutting against an individual's right to privacy under this subfactor. For commercial DNA data, consumers only submit a DNA sample to the commercial DNA network a single time.[117] This is completely unlike the cell-site data in *Carpenter* that was collected multiple times daily.[118] On the other hand, commercial DNA data fulfills the *length of data recordation* component of this subfactor. Once data is submitted to a commercial DNA network, unless the consumer affirmatively opts out, the data remains indefinitely.[119] This extends well beyond the five-year holding period in the cell-site databases in *Carpenter* that was deemed sufficient for purposes of this subfactor.[120]

---

[112] *See supra* text accompanying note 79.
[113] Lee, *supra* note 110.
[114] Adam Rutherford, *How Accurate Are Online DNA Tests?*, SCI. AM. (Oct. 15, 2018), https://www.scientificamerican.com/article/how-accurate-are-online-dna-tests/.
[115] *Id.*
[116] *See supra* note 79.
[117] Letzter, *supra* note 3.
[118] *See supra* text accompanying note 82.
[119] I myself have submitted DNA to 23andMe back in 2013, and I continue to receive updates on my data to this day.
[120] *See supra* text accompanying note 83.

Regarding "comprehensiveness," commercial DNA networks fulfill this subfactor by having more than 26 million members in their databases.[121] Despite never outlining a particular figure in its opinion, a number of this magnitude will more than likely be deemed "comprehensive" in reach for data privacy purposes.

The depth, breadth, and comprehensiveness of commercial DNA data are ambiguous. There are strong arguments on both sides for how much the data fulfills the characteristics described by this second *Carpenter* factor. Though a more conservative Court is likely to articulate the arguments against holding an individual right to privacy in commercial DNA, the information collected from this data would likely pass this second factor of the test.

3. Commercial DNA Data Collection Is Neither Inescapable nor Automatic

If there is any *Carpenter* factor that commercial DNA data will fail under, it is the "inescapable and automatic nature of collection." Nothing about commercial DNA data collection is inescapable nor automatic. A conservative Supreme Court will not extend *Carpenter*'s protections to commercial DNA data for this very reason.

In *Carpenter*, the inescapability of the cell-site data collection was tied to the fact that the Court believed, in modern society, a cell phone is essential for a functioning member of society.[122] Some scholars who support a right to privacy in commercial DNA data argue that *Carpenter* set the stage for anticipating "sophisticated systems that are already in use or in development."[123] In particular, these scholars envision a world where genetic testing and DNA submission are an inevitable necessity that become an expected norm in life; thus, like the cell phone, they become "inescapable" in nature and ought to receive privacy protection.[124] This world may very well be on its way, but this proposition discusses a different type of DNA data. DNA data submitted explicitly for health or diagnostic reasons is different from commercial DNA data submitted to networks like 23andMe and Ancestry.com. With commercial DNA networks, users take an *affirmative*[125]

[121] Regalado, *supra* note 2.
[122] *See supra* text accompanying note 88.
[123] Ram, *supra* note 97, at 1389.
[124] *See id.*
[125] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (discussing that cell-site data collection had not "*affirmative* act on the part of the user beyond powering up") (emphasis added).

and *voluntary* step to submit their DNA to a company seeking profit. There is nothing that draws these consumers to commit this action besides curiosity and interest in learning their DNA's heritage. Should a society arise where submitting DNA becomes a norm that is necessitated by the way of life, then *Carpenter*'s protection may apply, but this is not the case with how commercial DNA networks work today.

Other scholars push back on DNA submissions' "voluntariness" with regards to commercial DNA networks. To them, a voluntary action is synonymous with a "deliberate" action, which requires "full consciousness of the nature of one's act."[126] "A decision made with no appreciation for the risks is not truly a voluntary choice."[127] If a decision is not voluntary, then it is inescapable. The argument here is that consumers do not truly understand the risks associated with submitting their DNA to commercial networks.[128] In support of this claim, public opinion is cited showing that 91% of participants in commercial DNA networks believe police should be able to search genealogical websites in order to match DNA with potential violent crime suspects.[129] In other words, the argument goes, these individuals do not understand the privacy implications associated with DNA data and are therefore freely abandoning the data to potentially dangerous outside parties.[130] Because these risks are not understood by the general public, the argument concludes that the data is not truly "voluntarily" and "deliberately" given up; thus, its collection is automatic and inescapable and should be protected under the right to privacy.

There is nothing in *Carpenter* to suggest that data handed over to a third-party need be "deliberate" in order to lose privacy protection, but for argument's sake, even assuming that a voluntary action must be "deliberate," commercial DNA data would *still* fail under this factor. There is no doubt that the privacy concerns associated with new technologies are unknowns to the public during the technology's infancy period.[131] However, there must come a tipping point where the public's awareness becomes realized. Showing that 91% of participants in commercial DNA networks are content allowing police to search the database to solve crime does not necessarily mean that

[126] Baldwin, *supra* note 7, at 169.
[127] *Id.* at 170.
[128] *Id.* at 169–70.
[129] *Id.* at 175.
[130] *See id.* at 176.
[131] This has always been true, dating back to photography and breach of privacy discussed by Justice Brandeis. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

they do not understand the privacy risks involved with the data. Recent studies show that many Americans (77%) are extremely concerned with the rise of crime in cities across the country.[132] Combatting this rise in crime may be an issue to many that outweighs the low risk of one's own breach of privacy. This would logically explain the mindset of many commercial DNA network consumers.

Moreover, scholars should not patronize the public. The tipping point of awareness regarding data privacy has long passed. The majority of commercial DNA network users have a degree in higher education (at least a college degree).[133] Additionally, recent data suggests that 79% of Americans are concerned about how companies in general use their data and how it is collected.[134] Even if the consumer does not understand the intricate details of how data privacy breaches could harm them,[135] they are definitely aware of the privacy risks involved in using these companies. Despite this awareness, these consumers take an affirmative step to submit their data to commercial DNA networks hoping to learn more about themselves and their families. This action is voluntary, and yes, even deliberate because they are "aware of the consequences of giving DNA data to third parties."[136] Nothing about this transaction is "inescapable."

Commercial DNA data is also not collected "automatically." Unlike the cell-site data that is collected continually throughout the day when the user opens certain apps, sends texts, or makes calls,[137] commercial DNA networks, generally, offer users an ability to opt out.[138] In *Carpenter*, the

---

[132] *See* Julia Manchester, *Poll: Majority Say They Are Concerned About Rising Crime in US Cities*, THE HILL (July 27, 2020, 12:50 PM), https://thehill.com/homenews/campaign/509185-majority-say-they-are-concerned-about-rising-crime-in-us-cities-poll.

[133] 73.4% of commercial DNA network consumers who participated in a survey had at least a college degree. Lu J. et al., *Genetics Test Users Demographics and Psychographics*, WONDER (Oct. 19, 2019), https://askwonder.com/research/customer-demographics-genetics-test-users-demographics-psychographics-y1eh9pngj.

[134] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RES. CTR. (Nov 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[135] *Id.*

[136] Baldwin, *supra* note 7, at 175.

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

[138] *See, e.g.*, *Your Privacy Comes First*, 23ANDME (2020), https://www.23andme.com/privacy/?nav2=true&sub=ver1 (outlining a consumer's option on what they can do with the DNA data).

Court was particularly uneasy about the fact that "[a]part from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data."[139] This is absolutely not the case here. Consumers can still enjoy the benefits of these commercial DNA networks while also having access to an opt-out function should they choose to no longer be a part of the system.

With the already prevalent difficulty of extending *Carpenter* to new technologies, a conservative Supreme Court will not hold that commercial DNA data deserves protection in part because collection of said data is neither "inescapable" nor "automatic."

4. Predictive Summary

The *Carpenter* factors do not provide a clear-cut answer on whether a right to privacy exists in commercial DNA data. The previous sections argue that, when applied, the *Carpenter* factors strongly suggest that commercial DNA data does *not* receive the protections provided by the right to privacy. However, the ambiguity present in the analysis begs for the consideration of extrinsic factors, such as recently applied precedent and the future composition of the Supreme Court.

Recent precedent has avoided extending *Carpenter* to other technologies, seemingly waiting on the Supreme Court to make these determinations.[140] In light of the reasoning discussed in *Moore-Bush* and *Gayden*, the various circuit courts will not extend the right to privacy to commercial DNA data. For example, in *Moore-Bush*, the First Circuit's narrowing of the *Carpenter* doctrine to "public movements"[141] likely limited its applicability to commercial DNA data. Access to commercial DNA data does not grant the finder any information about the consumer's particular physical movements, especially as compared to the continual surveillance provided by the cell-site data in *Carpenter*. Based on this reasoning, the First Circuit would be hesitant to protect commercial DNA data under *Carpenter*. The reasoning in *Gayden* from the Eleventh Circuit likewise would inhibit the extension of *Carpenter* to commercial DNA data. Recall in that case, the Eleventh Circuit found that prescription drug data was not "intimate" enough to earn protection.[142] If prescription drugs, capable of instantly illuminating

[139] 138 S. Ct. at 2220.
[140] *See supra* Part II.C.
[141] *See supra* text accompanying note 94.
[142] *See supra* text accompanying note 96.

what diseases and disorders an individual patient possesses, are not "intimate," then the Eleventh Circuit would surely come to the same conclusion for a mere string of nucleotides in commercial DNA data.

The future of the Supreme Court likewise presents context that suggests that *Carpenter* will not be extended to commercial DNA data. By stressing that the decision was "a narrow one" meant to adapt to innovation in order to "ensure that [the Court does] not 'embarrass the future,'" Chief Justice Roberts left the door open for applying the doctrine in unique ways to different technologies.[143] Whether or not Chief Justice Roberts defects to the liberal side in a future commercial DNA privacy case is irrelevant. The decision will likely hinge on the newly appointed Justice Barrett.[144] Justice Barrett was not even willing to extend *Carpenter* to *cell phone data* in *Wanjiku*.[145] Therefore, finding privacy rights in a completely distinguishable technology from *Carpenter*, like commercial DNA data, will prove even more unlikely. Similarly, her rulings against *consumer* privacy, as in *Gadelhak*,[146] show her hesitancy in holding privacy rights in favor of consumers. Rather, it seems that Justice Barrett would more likely favor corporations like 23andMe and Ancestry.com in cases involving rights to privacy.

In conclusion, the Supreme Court is unlikely to hold that a privacy interest exists in commercial DNA data: (1) the *Carpenter* factors do not map onto this type of data and do not protect this information collection; (2) recent precedent suggests that courts are generally hesitant to extend *Carpenter*; and (3) a more conservative Supreme Court will not wish to extend *Carpenter* beyond its constraints.

B. Arguing in the Alternative: A Good-Faith Medical Research Exception

If laws are enacted to protect individual privacy in commercial DNA data,[147] a good-faith exception should be included for parties conducting

[143] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
[144] *See supra* text accompanying note 56.
[145] *See supra* text accompanying note 58.
[146] *See supra* text accompanying note 59.
[147] Statutory exceptions are quite common, and states should incorporate this exception in statutes like California's Consumer Privacy Act of 2018. *See supra* text accompanying note 50.

medical research; likewise, if the Supreme Court holds a similar privacy interest, they too should carve out this exception in the doctrine.

Exceptions in the law are commonplace.[148] More importantly, a good-faith exception to the right to privacy for Fourth Amendment purposes already exists for law enforcement. Under the good-faith exception to the exclusionary rule, if police officers obtain information under an *objectively reasonable good-faith reliance* on a search warrant, that information does not get privacy protection and is admissible in court.[149] For data privacy interests in commercial DNA data, a similar good-faith exception should exist that allows parties to access said data for medical research purposes. The proposed standard would require the following: (1) the party must be of the type that possesses ordinary skill in the medical research field; (2) the party must show efforts of good faith that include steps taken to maximize the security and anonymity of individuals who have contributed to the database; and (3) the party must show concrete steps taken to benefit society, including reducing the cost of drugs to consumers.

A common pattern that is noticeable when courts develop exceptions to doctrine, and similarly, when these exceptions are codified by statute, is a reliance on an objective party: the "reasonable person." Consider in tort law, for example, the "reasonable child" standard for negligence. This standard exempts children from being held to the traditional reasonable standard of care of an adult and, instead, compares a child's actions to the conduct of other children with like age, experience, and intelligence.[150] The first prong of the medical research good-faith standard devises a similar requirement. The party that uses commercial DNA data must have the requisite skillset needed to derive the potential benefits from the dataset. In patent law (the legal field most relevant to burgeoning technology), this skillset is referred to as "ordinary skill in the art."[151] Factors to consider for this prong include the

[148] Examples include the collateral order exception to the final judgment rule, the market participant exception to the constitutional ban on state protectionism, and the state action exemption in antitrust law. Frederick Schauer, *Exceptions*, 58 U. CHI. L. REV. 871, 871–72 (1991).

[149] United States v. Pope, 467 F.3d 912, 916 (5th Cir. 2006).

[150] *Negligence and the 'Reasonable Person'*, FINDLAW, https://injury.findlaw.com/accident-injury-law/standards-of-care-and-the-reasonable-person.html (last updated Nov. 30, 2018).

[151] Joseph P. Meara, *Just Who Is the Person Having Ordinary Skill in the Art? Patent Law's Mysterious Personage*, 77 WASH. L. REV. 267, 267 (2002) (introducing the concept of the person having ordinary skill in the art and comparing it to the reasonable person in tort law).

educational level of the party (e.g., possessing a graduate degree in biomedical sciences, engineering, etc.) and the typical expertise of members of the trade (e.g. extrinsic evidence and testimony from other pharmaceutical and medical researchers).[152] Further, one of ordinary skill in this art would need to demonstrate that the agreements they made with commercial DNA networks are similar to those accepted in the field. The purpose of this prong is to legally ensure that the exception only applies to those who have the applicable skillset to responsibly use commercial DNA data.

The second prong of the proposed standard is meant to encourage parties, particularly larger corporations like pharmaceutical companies, to invest in technologies and security systems that can defend against the privacy concerns associated with commercial DNA data. If an exception is going to allow parties to access commercial DNA data without legal fear of infringing on individual privacy rights, then these parties must show a genuine effort in preventing these privacy risks from manifesting. An example of efforts that could fulfill this prong would be to work with startups like Nebula. Nebula's mission is to provide a genomic service with enhanced privacy standards for its customers.[153] It has improved data security effectively by using split decryption keys (i.e., codewords) when sharing consumer data with other companies.[154] Partnerships with these types of companies would support this second prong of the exception.

The final prong of the proposed standard aims to supplement public policy. Exceptions to laws are almost always policy driven in order to maintain some social norm or expectation that, at least in theory, a majority of the public would support.[155] The extensive cost of drug production, stemming from upfront clinical trial costs as well as from high drug failure rates, trickles down unfairly to consumers who desperately need these drugs to live healthy lives.[156] This proposed good-faith exception would be utterly useless for the public if pharmaceutical companies did not take steps to actually reduce drug costs on the consumer. These parties must show some

---

[152] *See id.* at 286–90.

[153] Keren Landman, *Anonymous DNA Testing Is Here. But Who Wants It?*, ELEMENTAL (Oct. 9, 2019), https://elemental.medium.com/anonymous-dna-testing-is-here-but-who-wants-it-c642845fee1d.

[154] *Id.*

[155] *See, e.g.*, Richard L. Alfred & Ben T. Clements, *The Public Policy Exception to the At-Will Employment Rule*, 78 MASS. L. REV. 88, 88–89 (1993) (describing the exception to the at-will rule that prevents employers from terminating employees for reasons that go against public policy).

[156] *See supra* text accompanying notes 25–27, 34–38.

form of beneficial financial transfer: millions of dollars in savings arising from reduced failure rates and clinical trial costs due to commercial DNA data utilization need to be offset by at least *some* cost savings for the consumer.[157]

Critics of this good-faith exception will emphasize the consumer privacy risks, including those previously articulated in this Article, if pharmaceutical companies are allowed access to commercial DNA networks. Such privacy risks would include the potential for unfair uses of commercial DNA by law enforcement or the possible escalation of discrimination in the workplace stemming from DNA network data breaches.[158] These critiques are warranted, but excessive. As a society, we have reached a boiling point of suspicion against technological companies and the potential privacy risks they pose.[159] It seems everywhere one looks, the fears of "big tech" are stressed. At some point, such extreme caution will hinder progress. Of course, like all innovative technologies, commercial DNA networks have consumer privacy risks. This good-faith standard explicitly tries to *combat* these risks in the second prong. Further, the actual risk of the technology is minute when compared to the potential benefits these networks offer society in health and medicine.[160] To continue encouraging progress, a good-faith standard such as this one should be adopted in order to grant legitimate researchers a freedom from the fear of liability.

In conclusion, if parties can show they (1) have the skill required in the field, (2) have made genuine efforts to combat privacy risks in commercial DNA data, and (3) have made concrete steps to reduce drug costs on consumers, they should be legally allowed to access commercial DNA data to conduct medical research.

---

[157] *See* Ledesma, *supra* note 26.

[158] *See supra* text accompanying note 105.

[159] *See supra* text accompanying notes 129–136.

[160] Recall that the deanonymization of DNA data is extremely difficult and, even if completed, its analysis would require a level of skill of a computational biologist. *See supra* text accompanying note 112. On the other hand, the significant benefits in clinical trial cost reduction and medical research have already been observed through these DNA networks. *See supra* Part I.A.2.

CONCLUSION

Commercial DNA networks are supremely popular, and their popularity will continue to grow. With this established technology comes potential privacy concerns for consumers along with potential health benefits for society as a whole. Based on the factors laid out in the holding of *Carpenter v. United States*, recent precedent, and the future of the Court, the Supreme Court will not hold that a privacy interest exists for individuals' DNA submitted to commercial networks. Regardless of what the Court or the states decide, the potential advantages that arise from access to these commercial DNA networks should lead to a good-faith exception for parties seeking to access these databases for medical research.

* * *