THE INTIMATE NATURE OF DNA IN CRIME-SOLVING

Jade W. Sobh[1]

I. INTRODUCTION

In *Carpenter v. United States*,[2] the Supreme Court held that law enforcement officials may no longer retrieve the cell-site location information from cell network carriers without first obtaining a warrant.[3] The Court ruled that collection of this information was protected by the

[1] J.D. Candidate, 2020, Seton Hall University School of Law. B.A. 2017, George Washington University. Thank you to all of those who encouraged me to keep thinking, learning, and advocating for what I believe in. My family, my teachers and professors, my friends and fellow law students, and the faculty at the law school have all been instrumental in my growth as an aspiring attorney. I hope to one day impart the same wisdom onto those after me.

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

[3] *Id.* at 2221.

Fourth Amendment due to the sensitive nature of location tracking.[4] Prior to *Carpenter*, prosecutors could acquire location information from carriers without a warrant because courts found that suspects had voluntarily given the information to their cellular network carrier, thereby depriving the location information of its subjective privacy interest.[5] In the realm of genetic information and its use in criminal investigations, law enforcement officials can use DNA in a variety of ways and may acquire it covertly, consensually, by force, or from family members.[6] Because there is no privacy interest in abandoned property or voluntarily revealed information, law enforcement officials have circumvented privacy interests in genetic data by claiming that a person who exposes their DNA to a company or website that collects and analyzes DNA (such as Ancestry.com or 23&Me) has somehow undermined their privacy interest in their own genetic information.[7]

While *Carpenter* concerned the government's acquisition of cell-site location services, its rationale regarding the government's general acquisition practices can also apply to the acquisition and use of DNA information. This rationale could call for future regulatory legislation to require a warrant to acquire and use a suspect's genetic information. This comment will show that genetic information deserves special protection due to its sensitive and immutable nature, and that new regulations should be promulgated to effectively protect the citizenry from a "too permeating police surveillance."[8] Part II will analyze all of the ways in which police currently use genetic information and under what circumstances genetic information is protected. Part III will examine the implications of exposing an individual's genetic information, and the interest in keeping that information private and protected. Part IV will look to the Supreme Court's decision in *Carpenter* to determine how to effectively regulate law enforcement's acquisition and use of DNA in solving crimes.

---

4 *See id.* at 2221–22.

5 *See id.* at 2216.

6 *See* Edward J. Imwinkelried & D.H. Kaye, *DNA Typing: Emerging or Neglected Issues*, 76 WASH. L. REV. 413 (2001).

7 *See* Gina Kolata & Heather Murphy, *The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder*, N.Y. TIMES (April 27, 2018), https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html.

8 *Carpenter*, 138 S. Ct. at 2231.

II. HOW LAW ENFORCEMENT UTILIZES DNA

A. What Justifies Police Collection of an Arrestee's Genetic Information?

In 2013, the Supreme Court decided *Maryland v. King*,[9] and granted law enforcement across the nation the ability to save the DNA of arrestees—arrested wrongly or otherwise—to the Combined DNA Index System (CODIS), where it can be used to identify suspects in past crimes, future crimes, or cold cases.[10] In DNA testing, the coding regions are known as genes and contain the information necessary for a cell to make proteins, but non-protein-coding regions are not related directly to making proteins and have been referred to as "junk DNA."[11] The Supreme Court stated that "junk DNA" contains no "far reaching and complex characteristics like genetic traits."[12]

In *Maryland v. King,* Alonzo King was arrested for first and second degree assault and was compelled by police officers to participate in a "buccal swab" of the inside of his cheeks.[13] At the time, under the Maryland DNA Collection Act, a DNA sample must have directly related to "the identification of individuals" involved in the crime, and an officer was not permitted to "perform a search of the statewide DNA database for the purpose of identification of an offender in connection with a crime for which the offender may be a *biological relative*."[14] In the context of Fourth Amendment protection, the Court held that "a buccal swab on the inner tissues of a person's cheek in order to obtain DNA samples is a search."[15] But the Fourth Amendment's proper function is to defend against "intrusions which are not justified in the circumstances, or which are made in an improper manner."[16] The "ultimate measure" of the constitutionality of a governmental search is reasonableness, and the Court found the "buccal

---

9 569 U.S. 435 (2013).

10 *Id.* at 441.

11 *Id.* at 442.

12 *Id.* at 442-43.

13 *Id.* at 440 ("As part of a routine booking procedure for serious offenses, his DNA sample was taken by applying a cotton swab or filter paper . . . to the inside of his cheeks.").

14 *Id.* at 444 (emphasis added) (citing Md. Code Ann. Pub. Safety § 2-506(d)).

15 *King*, 569 U.S. at 446 ("The Court has applied the Fourth Amendment to police efforts to draw blood, scraping an arrestee's fingernails to obtain trace evidence and even to a breathalyzer test.") (internal citations omitted).

16 *Id.* at 447 (quoting Schmerber v. California, 384 U.S. 757, 770 (1966)) (internal quotations omitted).

swab . . . falls within this category."[17] But even if a warrant is not required, a search "must be reasonable in its scope and manner of execution," and the Court balanced the "privacy-related and law enforcement-related concerns to determine if the intrusion [was] reasonable."[18]

The government in *King* argued that it had an interest in collecting arrestees' DNA to (1) identify the arrestee, (2) guarantee the safety of police officers, (3) ensure the persons accused are available for trials, (4) know an individual's past conduct and accurately determine bail, and (5) aid in crime solving and possibly free persons wrongly imprisoned.[19] The Court then weighed these interests against the privacy-related interests of DNA collection by examining technology's evolution and use in solving crimes, while making reference to other means of identification such as "photographing and fingerprinting."[20] The Court acknowledged that "DNA identification is an advanced technique superior to finger-printing in many ways" but the Court stated "[t]he additional intrusion upon the arrestee's privacy is not significant," so it gave great weight both to the significant government interest at stake in the identification of arrestees, and to the unmatched potential of DNA identification to serve that interest.[21]

The Court in *King* explained that the arrestee's privacy-related interest is "a minimal one."[22] The reasonableness of any search "must be considered in the context of the person's legitimate expectations of privacy," and the Court noted "the expectations of privacy of an individual taken into police custody 'necessarily [are] of a diminished scope.'"[23] The Court distinguished the diminished privacy interests of arrestees and the search at issue in the case from "the sort of programmatic searches of . . . the public at large," which might have a heightened expectation of privacy.[24] But, in the absence of individualized suspicion, the Court has insisted on the search having "some purpose other than to detect ordinary criminal wrongdoing" to justify the search as necessary.[25] The Court held that individualized suspicion was not categorically required for *King* because of his "diminished expectations of privacy" and because the intrusion was "minimal."[26] The Court closed its opinion by reiterating that the defendant's DNA is used only for identification, that CODIS did not reveal the genetic traits of the arrestee

17 *Id.* at 448.
18 *Id.* (citing Illinois v. McArthur, 531 U.S. 326, 331 (2001)).
19 *Id*. at 449-56.
20 *Id*. at 459.
21 *King*, 569 U.S. at 459-61.
22 *Id.* at 461.
23 *Id.* at 462 (quoting Bell v. Wolfish, 441 U.S. 520, 557 (1979)).
24 *Id.*
25 *Id.* at 463 (internal quotations omitted).
26 *Id.* at 463.

(just his "junk DNA"), and the Court reassured readers of its opinion that the Maryland DNA Collection Act guards against further invasions of privacy.[27]

King established that arrestees have a more limited scope of privacy interests than suspects of crimes, but the Court only saw DNA for its productive use in identification, comparing it to categorically different information such as photographing or fingerprinting, and thereby failed to see its potential for exposing private information. The Court mischaracterized non-coding regions of DNA as "junk DNA" when there is in fact sensitive information available in non-coding regions.[28] The remainder of Part II will discuss the potential risks associated with the exposure of sensitive genetic information, but it is necessary to understand how the Supreme Court's characterization of genetic information has set the foundation for the current lack of protection in DNA collection and analysis.

B. What Justifies Law Enforcement Collection of Genetic Information from Suspects?

1. Voluntary Exposure of Genetic Information

While arrestees have a diminished expectation of privacy, mere criminal suspects retain the full body of constitutional protections.[29] The Fourth Amendment protects against "police efforts to obtain samples directly from suspects," but that prohibition only applies to government action, leaving open the possibility that "the police may be able to acquire preexisting information from cooperative private hospitals or laboratories without a court order and without probable cause or reasonable suspicion."[30] This would rely on the fact that the individual provided the third party with the information, stripping it of its privacy interest, and allowing the government to avoid engaging in any search or seizure.[31]

This loophole acts as a work-around people's privacy rights. What is constitutionally protected by the Fourth Amendment relies both on what a person's actual subjective expectation of privacy is, as well as whether that expectation is one that society is willing to accept as reasonable.[32] In the seminal privacy case, *Katz v. United States*,[33] the government acquired evidence by attaching a recording device to a phone booth and argued that there was no search because there was no *physical* trespass, and because the

---

27 *King*, 569 U.S. at 464-65.

28 *See* Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 881 (2015).

29 *King*, 569 U.S. at 462.

30 Imwinkelried & Kaye*, supra* note 6, at 425.

31 Imwinkelried & Kaye*, supra* note 6, at 425.

32 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

33 *Id.* at 348–49.

phone booth was a public place. The Court ruled, and Justice Harlan's concurring opinion further extrapolated, that because the federal agents had no warrant authorizing the interception, the search violated the Fourth Amendment and warrantless searches are per se unreasonable, subject to some exceptions.[34] Justice Harlan explained that "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[35]

Subsequently, the Supreme Court applied the *Katz* test in *United States v. Miller,*[36] and found that Miller, charged with possessing an unregistered still, was evading taxes.[37] The bank cooperated with law enforcement by surrendering information and records on Miller's account, and Miller moved to suppress the documents on the ground that he made the information available to the bank for a "limited purpose."[38] The Court rejected this argument on the grounds that Miller had taken the risk to reveal his affairs and that he understood they might be conveyed to the government.[39] The Court noted that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and [that] the confidence placed in the third party [would] not be betrayed."[40]

Professor Imwinkelried and Professor Kaye have identified three bases to distinguish *Miller* from cases involving DNA: (1) *Miller* involved bank records concerning commercial transactions, not DNA, which contains intimate and private medical information; (2) even if *Miller* applies to medical *documents*, it probably does not apply to a physical DNA sample because the sample represents a greater threat to privacy on account of the ability to derive much more—possibly unrelated—private information; and (3) where *Miller* voluntarily conveyed the information to the bank, law enforcement's "voluntary" acquisition of DNA is debatable depending on the circumstances.[41]

2. "Abandoned" DNA

DNA may be covertly taken by police by following "a bread-crumb

34 *Id*. at 357.
35 *Id*. at 361 (Harlan, J., concurring).
36 United States v. Miller, 425 U.S. 435, 442 (1976).
37 *Id.* at 436; Imwinkelried & Kaye, *supra* note 6, at 427.
38 Imwinkelried & Kaye, *supra* note 6, at 427; *Miller*, 425 U.S. at 442.
39 *Miller*, 425 U.S. at 443.
40 *Id*.
41 Imwinkelried & Kaye, *supra* note 6, at 429-31.

trail of identifying DNA matter."[42] According to current law and regulation, an individual who has "abandoned . . . [genetic] material in a public place, retains no reasonable expectation of privacy in it."[43] Currently, "[c]onstitutional law offers virtually no protection to suspects who are targeted for their abandoned DNA," and "existing Fourth Amendment law is ill-suited to the facts of abandoned DNA collection."[44] As stated above, police activity "constitutes a 'search' for Fourth Amendment purposes only if the person claiming an illegal search exhibits both an actual expectation of privacy and one that 'society is prepared to recognize as "reasonable."'"[45] While acquiring a person's DNA by force would constitute a search, "where suspects 'knowingly expose' items to public view, the Court has held that the collection of such evidence falls outside the Fourth Amendment's protections."[46]

Most people would not think that throwing away a water bottle, hairbrush, or toothbrush means you are giving up your right to privacy in your DNA, but under the current understanding, that is exactly what it means. Viewing DNA as "abandoned" is untenable because its emission or emanation in public places cannot be avoided—and this is true whether it is hair, saliva, or any other involuntarily secreted material containing genetic information.[47] Legal scholars have found that "the Fourth Amendment query focuses on the item left behind—usually of no concern to the person targeted—rather than the genetic information contained within it," so, as applied, "the Fourth Amendment fails to protect genetic privacy adequately."[48] While the Supreme Court has found that garbage may not maintain a privacy interest since it has been abandoned and left for collection, DNA is clearly different because "one can shred papers or burn garbage . . . but leaving DNA in public places cannot be avoided."[49] Therefore, the analogy of DNA to trash may not be the most productive or accurate. Some have put forth other analogies for DNA, comparing it to fingerprints, the body and its organs, or human waste; meanwhile, others have advocated for genetic exceptionalism.[50] While the Court in *King*

---

42 United States v. Kincade, 379 F.3d 813, 873 (9th Cir. 2004) (Kozinski, J., dissenting).

43 Imwinkelried & Kaye, *supra* note 6, at 437.

44 Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. U.L. REV. 857, 863 (2006).

45 *Id*. (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

46 *Id*. (quoting *Katz*, 389 U.S. at 351).

47 *Id*. at 867.

48 *Id*. at 866.

49 *Id*. at 867.

50 Joh, supra note 44, at 868–74. Genetic exceptionalism is the belief that genetic information is special and so must be treated differently from other types of medical data or other personally identifiable information.

compared the use of DNA for identification to the use of fingerprints, this comparison is shaky at best. As Justice Scalia noted in his dissent, "the Court's comparison of Maryland's DNA searches to other techniques such as fingerprinting, can seem apt only to those who know no more than today's opinion chose to tell them about how those DNA searches actually work."[51]

As technology evolves, we are deriving increased information from DNA. As Part II will explain in detail, our previous scientific understanding of DNA has changed since *King*, and 'junk' DNA is no longer a term used to describe the DNA analyzed for identification because scientist *have* found private information in these parts of DNA.[52] Surely, the code that contains all of our genetic information—including predispositions to diseases, ancestral and racial backgrounds, private medical information, familial information, and information still to be deciphered—deserves more protection than the pattern found at the tips of our fingers used only for identification. Without further regulation and protection, Americans are allowing collection of some of the most sensitive information that exists about themselves, and all without a warrant. There is no comparable sensitive information that is not thoroughly protected by regulation or well-established privacy interest.

3. Familial DNA

Familial searching generally refers to looking in a DNA database not for the person who left the crime-scene sample, but rather for a relative of that person.[53] Understanding familial searches from a Fourth Amendment perspective is difficult and has not been attempted by the Supreme Court.[54] In *King*, the Court found that the *acquisition* of DNA constitutes a separate Fourth Amendment event from the *analysis* of the DNA, and many have speculated that the only manageable Fourth Amendment framework is to see these two as distinct searches.[55] Familial searches "fall between the cracks" because "even if the searching violated a right, it is not clear it would be the relative's right (and not the original database lead's)."[56]

A DNA sample "carries sensitive information about [an] individual—and . . . about the close relatives of [an] individual."[57] In the context of Fourth Amendment searches, "the convicted offender's diminished privacy

---

51 *King*, 569 U.S. at 466 (Scalia, J., dissenting).

52 Ram, *supra* note 28, at 881.

53 Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases,* 109 MICH. L. REV. 291, 297 (2010).

54 *Id*. at 333.

55 *Id*. at 335; *see also* Ram, *supra* note 28, at 896.

56 Murphy, *supra* note 53, at 334–35.

57 David H. Kaye, *The Genealogy Detectives: A Constitutional Analysis of "Familial Searching"* 50 AM. L. REV. 109, 137 (2013).

cannot in turn diminish the privacy of his or her relatives," because "the relative never 'assumed a risk.'"[58] This would be true whether the original DNA came from an arrestee in CODIS or from a non-criminal database. In both scenarios, the third party did not volunteer their DNA, and had no say in their family member's involuntary (or voluntary for genetic databases) exposure of shared genetic data.

Recent cases have brought this issue to the forefront of the genetic privacy debate. In April of 2010, investigators in California used familial searching to uncover a potential match in search of the "Grim Sleeper."[59] Using the information from the search—that came from the killer's convicted son—the police conducted a sting operation, and collected a discarded piece of pizza from the suspect's trash, which was tested and found to match the DNA found at the crime scenes.[60] The suspect was subsequently arrested.[61] Those who oppose familial searches of CODIS argue that it serves as a form of racial profiling because a higher population of inmates are minorities, and this gives the authorities an ability to filter by race and disproportionally toward minorities.[62] Jeffery Rosen, a law Professor at George Washington University, has stated that "the technique is not inherently good or evil," but rather that it has to do with "what crimes it is used for, who's in the database, how the database is regulated and what is done with the samples."[63]

Recently, the Golden State Killer was found in California using DNA technology and *non-governmental* DNA databases.[64] When the police found no matches in CODIS, they uploaded the DNA to a public DNA database website called GEDMatch.[65] Although GEDMatch discloses that profiles could be used to investigate violent crimes, many customers of genealogy companies did not realize they would be signing up to help criminal investigations.[66] The disclosures led to "49 genetic identifications" and the

---

58 Murphy, *supra* note 53, at 336.

59 Murphy, *supra* note 53, at 294.

60 Murphy, *supra* note 53, at 294.

61 Jennifer Steinhauer, *'Grim Sleeper' Arrest Fans Debate on DNA Use*, N.Y. TIMES (July 8, 2010), https://www.nytimes.com/2010/07/09/us/09sleeper.html.

62 *Id.*

63 *Id*.

64 Gina Kolata & Heather Murphy, *The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder,* N.Y. TIMES (Apr. 27, 2018), https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html.

65 *Id*.

66 Heather Murphy, *Sooner or Later Your Cousin's DNA Is Going to Solve a Murder*, N.Y. Times (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/us/golden-state-killer-dna.html.

reopening of a number of cold cases.[67] An additional 300 cases are in the process of being reopened: old murders, serial sexual assaults, and unidentified bodies, according to estimates by various genealogists and investigators.[68] Some believe that the same regulations imposed by states on CODIS should also be placed on family genealogy sites.[69] As this method is being used more and more, Americans are finding out that they have little to no recourse to protect their genetic data.[70] "In the hands of an advanced genealogical sleuth, often all that's needed to identify someone from a drop of saliva, blood, or semen are the DNA profiles of two third cousins."[71] This novel method of investigation requires analysis under the lens of the third-party doctrine of *Miller*, the DNA privacy interests in *King*, and a legal framework for familial searching in crime solving.

Genetic information is a powerful tool. Like any powerful tool, it can be used to make the world safer, or it can be used oppressively. In China, the government is using genetic information to track, oppress, detain, and control the minority population of Uighurs, a predominantly Muslim ethnic group.[72] Chinese Officials are saying that a comprehensive DNA database could be used to chase down any Uighurs who resist conforming to the Chinese campaign of "re-education" meant to make Uighurs more subservient to the Communist Party.[73] Dr. Kidd, a Yale Professor and a major figure in the American genetics field, said he had been "unaware of how his material and know-how were being used," and the scientific community is reeling from China's use of DNA databases.[74]

Imagine a world where the police or other government enforcement authority has the ability to find out private personal information about you by finding pieces of hair you shed, or by finding your saliva on a water bottle you discarded. Imagine a world where private genetic information about your predisposition to diseases or your ancestral history can be traced back to you, simply by a family member's decision to submit their own genetic information—even from a relative as distant as a third cousin. Police are not supposed to be interested in the personal information—such as health information or ancestry—within our DNA, and rather should only use it for

---

67 *Id*.

68 *Id*.

69 *Id*.

70 *Id*.

71 *Id*. (A third cousin is someone who shares a set of your sixteen great-great-great grandparents, which might consist of over 800 people).

72 Sui-Lee Wee, *China Uses DNA to Track Its People, With the Help of American Expertise*, N.Y. TIMES (Feb. 21, 2019), https://www.nytimes.com/2019/02/21/business/china-xinjiang-uighur-dna-thermo-fisher.html.

73 *Id*.

74 *Id*.

purposes of identifying individuals.[75] And while the police are only allowed to use this information for a limited purpose, genetic information is still extremely sensitive and completely immutable, and for that reason police should secure a warrant prior to obtaining and/or analyzing DNA. As some of the examples above demonstrate, the use of genetic information is evolving alongside our understanding of it. More safeguards are required to maintain the balance of power between the people's privacy interests and the government's interests in public safety. While the power of genetic information may be used for good, it can also be applied for nefarious purposes.

III. THE IMPLICATIONS OF BREACHING GENETIC PRIVACY

A. Why Protect Genetic Information?

Upon first glance, some might ask why people should even be concerned with the advancement of genetic technology and instead focus solely on its beneficial effect on crime solving. As Justice Scalia points out in his dissent in *King*, when America was still in its infancy, the British would use "general warrants," which were not grounded upon a sworn oath of a specific infraction, and therefore were not limited in scope and application.[76] The Virginia Constitution first addressed general warrants as "grievous and oppressive," and "the Maryland Declaration of Rights similarly provided that general warrants were 'illegal.'"[77] Worries about the uses of oppressive police powers lead to "Madison's draft of what became the Fourth Amendment."[78] While courts have found that there is a "closely guarded category of constitutionally permissible suspicionless [sic] searches," these searches were never meant to serve "the normal need for law enforcement."[79] Justice Scalia also made clear that "the legitimacy of the Court's method and the correctness of its outcome hinge entirely on the truth of a single proposition: that the primary purpose of these DNA searches is something other than simply discovering evidence of criminal wrongdoing."[80]

The Court in *King* attempted to maneuver around this requirement, finding that the buccal swab and DNA acquisition was for "identification" purposes, but "that seems . . . quite wrong—unless what one means by

---

75 Maryland v. King, 569 U.S. 435, 464–65 (2013)

76 *King*, 569 U.S. at 466 (Scalia, J., dissenting).

77 *Id*. at 466–67 (Scalia, J., dissenting).

78 *Id*. at 467 (Scalia, J., dissenting).

79 Chandler v. Miller, 520 U.S. 305, 309 (1997); Skinner v. Railway Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989) (internal quotation marks omitted); *King*, 569 U.S. at 467-68 (Scalia, J., dissenting).

80 *King,* 569 U.S. at 468 (Scalia, J., dissenting).

'identifying' someone is 'searching for evidence that he has committed crimes unrelated to the crime of his arrest.'"[81] Of course, if identifying someone means finding out what unsolved crimes he has committed, then "identification is indistinguishable from the ordinary law-enforcement aims that have never been thought to justify a suspicionless [sic] search."[82] Significantly, "King was not identified by his association with the [DNA] sample; rather, the sample was identified by its association with King," undermining the majority's "identification" theory.[83] In Justice Scalia's words, "it is safe to say that if the Court's identification theory is not wrong, there is no such thing as error."[84]

To further bolster its identification argument, the Court in *King* compares DNA to taking a person's photograph or fingerprints.[85] The Court, however, has never held that a person has an expectation of privacy in a photograph, nor that taking fingerprints is a Fourth Amendment search.[86] Unlike DNA, which is used solely to solve crimes, fingerprints are actually taken to identify arrestees and fingerprints do not contain the same level of information as DNA.[87] "Solving unsolved crimes is a noble objective, but it occupies a lower place in the American pantheon of noble objectives than the protection of our people from suspicionless [sic] law-enforcement searches."[88] Justice Scalia closed his dissent by rejecting the idea that "the proud men who wrote the charter of our liberties would have been so eager to open their mouths for *royal inspection*."[89]

If we determine that our current understanding of genetic information is inadequate, how might we reframe the way the law protects our genetic information, or how might we promulgate regulations on the government's access, storage, and use of our personal genetic information?

B. "Ownership" of DNA

One possible solution to the issue of shared genetic information is to treat shared DNA as protected by a theory similar to tenancy by the entirety.[90] In her article "DNA by the Entirety," Professor Ram explains two examples

---

81 *Id*. at 469–70 (Scalia, J., dissenting).

82 *Id*. at 470 (Scalia, J., dissenting).

83 *Id*. at 474 (Scalia, J., dissenting).

84 *Id*. at 476 (Scalia, J., dissenting).

85 *Id*. at 459.

86 *King,* 569 U.S. at 476–77 (Scalia, J., dissenting); *see also id.* at 458 ("fingerprinting did not violate the Fourth Amendment precisely because it fit within the accepted means of processing an arrestee into custody.").

87 *Id*. at 478 (Scalia, J., dissenting).

88 *Id*. at 481 (Scalia, J., dissenting).

89 *Id*. at 482 (Scalia, J., dissenting) (emphasis added).

90 Ram, *supra* note 52, at 877.

of familial DNA threatening privacy interests.[91] First, a member of the Lacks family died from cervical cancer and had their cells used for research resulting in the publication of that individual's genome.[92] Second, a man suspected of a crime was found by his relation to a family member who had also been arrested, and his DNA was "abandoned" and subsequently collected, resulting in a positive match and an arrest.[93] The three prominent areas affected by familial privacy interests in genetic data are forensic familial identification, genetic research, and personal genetic testing.[94] If identifiable genetic information is worthy of protection, "then legal institutions must take its inherently shared nature seriously."[95]

Because of the shared nature of DNA, an "individual's authority to control their 'own' identifiable genetic information may be affected by how the government, research entities, or genetic testing firms make use of genetic information drawn from close genetic relatives."[96] Unlike your social security number, credit card information, or bank account number, "the genetic information an individual inherits from her parents is the genetic information she will always have."[97] Given the immutable nature of genetic information, once it is exposed without your consent, "nothing can be done to sever your connections to that information," and both the individual and their family would have suffered invasions to their genetic privacy.[98] In the terms of a tenancy by the entirety, "the shared nature of identifiable genetic information is not subject to severance," and therefore deserving of higher scrutiny.[99]

Furthermore, genetic information is shared non-volitionally.[100] This is especially relevant in the context of "voluntarily shared" information. "Notions of abandonment, which play a key role in both research and forensic uses of genetic information . . . turn on some notion of volition—the 'knowing exposure' of material or information to the public."[101]

Some have postulated that "property offers a more advantageous lens for addressing shared interests in identifiable genetic information."[102] Through tenancy by the entirety, the law chooses to perceive two people as

91 Ram, *supra* note 28, at 874–75.
92 Ram, *supra* note 52, at 874.
93 Ram, *supra* note 52, at 875.
94 Ram, *supra* note 28, at 876.
95 Ram, *supra* note 28, at 877.
96 Ram, *supra* note 28, at 899.
97 Ram, *supra* note 28, at 903.
98 Ram, *supra* note 28, at 903.
99 Ram, *supra* note 28, at 904.
100 Ram, *supra* note 28, at 904.
101 Ram, *supra* note 28, at 905.
102 Ram, *supra* note 28, at 908.

one person at law, so that neither person owns any individual interest in an estate, rather it belongs to the couple.[103] "Genetic information among closely related individuals also exhibits a unity of identity, . . . a biological one."[104] Certain policy measures already acknowledge the shared nature of genetic privacy. The Genetic Information Nondiscrimination Act (GINA) extends medical privacy protection to "genetic information," and defines an individual's genetic data to include information about "the genetic tests of family members of such individual."[105] Some solutions, like one practiced in Iceland, include requiring the informed consent of family members before shared genetic information is exposed.[106]

As applied, this property theory of DNA would consider the State's use of DNA in familial searching an encumbrance, and tenancy by the entirety forbids encumbrance of shared property without the consent of the other partner.[107] The encumbrance would spread to any individual whose genetic information is exploited by the government's use.[108] As far as "forfeiture" of the property is concerned, the shared property is generally still protected, as it is owned by the other spouse.[109] In other words, "courts should constrain the government to using genetic information it has lawfully obtained to search for matches implicating the match offender—but not to search for matches implicating the matching offender's close genetic relatives."[110] Looking for an exact match only implicates the suspected offender's genetic privacy, and therefore does not breach the privacy of the suspect's close family members.[111]

C. Privacy as the Main Concern

Forensic analysis of DNA currently examines "variations in the lengths of . . . short tandem repeats (STRs) to construct DNA profiles."[112] STRs have medical implications, and can be used to identify inherited degenerative neurological disorders that could lead to diseases like dementia.[113] These forms of genetic variations appear in both coding and non-coding regions of

103 Ram, *supra* note 28, at 910.
104 Ram, *supra* note 28, at 911.
105 Ram, *supra* note 28, at 915–16; *see also* 42 U.S.C. § 300gg–91(d)(16) (2012).
106 Ram, *supra* note 28, at 901.
107 Ram, *supra* note 28, at 920.
108 Ram, *supra* note 28, at 920.
109 Ram, *supra* note 28 at 921–22.
110 Ram, *supra* note 28, at 923.
111 Ram, *supra* note 28, at 923.
112 Ram, *supra* note 28, at 880.
113 Ram, *supra* note 28, at 880; *see also* Karen Usdin, *The Biological Effects of Simple Tandem Repeats Lessons From the Repeat Expansion Diseases*, 18 GENOME RES. 1011 (2008).

the genome, but the STRs that American forensic labs typically examine are those located in non-coding portions of the genome.[114] Significantly, new research has cast doubt on the notion that non-coding DNA is "junk," and researchers have linked genetic disorders to STRs in non-coding regions of genes, suggesting the distinction between coding and non-coding regions are less rigid than previously thought.[115]

Direct-to-consumer companies like 23andMe distinguish the "individual level information" that they supply to customers from the "anonymized and aggregated information" that they share or sell to third parties.[116] "Individual level information" is information about a single individual's genotypes, diseases or traits/characteristics, which they "anonymize and aggregate" by stripping the genome of an individual's name and contact information before aggregating the information with others.[117] But recent studies have demonstrated that "anonymization" may not be possible.[118] Anonymization may not be possible because an individual can be uniquely identified with access to just seventy-five single-nucleotide polymorphisms (SNPs), while genome-wide association studies routinely use more than 100,000 SNPs to genotype individuals.[119] Re-identification is possible even from pooled or aggregated DNA data and often yields information about both the specific individual from whom the genetic material came, and her close genetic relatives.[120]

Congress has demonstrated an understanding of the importance of genetic information through passage of the Genetic Information Nondiscrimination Act (GINA).[121] GINA "aims to protect individuals from discrimination on the basis of genetic information in the employment and health insurance markets."[122] GINA "clarifies that 'genetic information' is 'health information' under the Health Insurance Portability and Accountability Act of 1996 (HIPAA)."[123] HIPAA emphasizes the need for control "where 'individually identifiable' information is at issue."[124] The HIPAA definition depends on the "identifiable" nature of the information,

114 Ram, *supra* note 28, at 880.

115 Ram, *supra* note 28, at 881.

116 Ram, *supra* note 28, at 886.

117 Ram, *supra* note 28, at 886.

118 Ram, *supra* note 28, at 886; s*ee also* Jeantine E. Lunshof et al., *From Genetic Privacy to Open Consent*, 9 NATURE REVS. GENETICS 406, 406 (2008).

119 Ram, *supra* note 28, at 886; Amy L. McGuire & Richard A. Gibbs*, No Longer De-Identified*, 312 SCIENCE 370, 370 (2006).

120 Ram, *supra* note 28, at 886–87.

121 Genetic Information Nondiscrimination Act of 2008, 110 Pub. L. No. 233, 122 Stat. 881 (2008).

122 Ram, *supra* note 28, at 894.

123 Ram, *supra* note 28, at 895.

124 Ram, *supra* note 28, at 895.

so companies anonymize genetic data to be excluded from the definition, but as this paper has already established, anonymous data has been re-identified and therefore cannot be excluded from the HIPAA definition.[125]

As stated earlier in Part II, in *King*, the Supreme Court recognized that "the *analysis* of identifiable genetic information, and not only its collection, calls for constitutional scrutiny—and thus that identifiable genetic information is information in which individuals may have a legitimate expectation of privacy."[126] While the Court concluded that neither collection nor analysis is impermissible under the Fourth Amendment where an individual has been validly arrested for a serious crime, it is significant "that the Court considered the genetic analysis independently, as it implies that genetic analysis itself implicates a privacy interest of constitutional magnitude."[127] While the privacy interest in that information will not necessarily stop the government from making use of that information without authorization, the "existence of that interest demands more searching scrutiny where unauthorized or compelled genetic analysis is at issue."[128] The differentiating factor in the *King* decision was the Court's finding of a diminished expectation of privacy based on King's status as an arrestee.[129] The Court in *King* was also under the impression that the information it claimed to be using for identification purposes was "junk," while we now know that is not the case—making the comparison to fingerprints or photographs inapposite.[130] "In sum, policymakers, courts, and ordinary citizens agree: enabling individuals to control dissemination of their identifiable genetic information—whether in the language of privacy or property—is worthy of pursuit."[131]

IV. HOW *CARPENTER* MIGHT AFFECT THE USE AND COLLECTION OF GENETIC INFORMATION

A. Carpenter and the Third-Party Doctrine

In *Carpenter v. United States,*[132] the Supreme Court held that: (1) the government acquiring an individual's historical cell-site location information (CSLI) from wireless carriers constituted a search under the Fourth Amendment, and that the search invaded an individual's reasonable

125 Ram, *supra* note 28, at 895.
126 Ram, *supra* note 28, at 896 (emphasis added).
127 Ram, *supra* note 28, at 896.
128 Ram, *supra* note 28, at 896.
129 Maryland v. King, 569 U.S. 435, 462 (2013).
130 *Id.* at 442-43.
131 Ram, *supra* note 28, at 897.
132 138 S. Ct. 2206 (2018).

expectation of privacy in the whole of his movements, despite the fact that the government obtained the information from a third party; and (2) a court order obtained by the government under the Stored Communications Act was not a permissible mechanism for accessing historical CSLI because it fell short of probable cause—therefore requiring a warrant.[133]

Timothy Carpenter was picked up by police concerning a number of robberies that had occurred in the Detroit area.[134] The police applied for a court order, based on information given by the suspect, to obtain cell phone records from Carpenter's wireless carriers under the Stored Communications Act.[135] The cell phone records provided the government with 12,898 location points cataloguing Carpenter's movements, averaging out at about 101 per day.[136] Carpenter challenged the evidence with a motion to suppress the CSLI, which he argued was obtained without a warrant supported by probable cause, but the district court denied the motion.[137] "The Sixth Circuit Court of Appeals affirmed, holding that Carpenter lacked a reasonable expectation of privacy in the location information . . . because he had shared that information with his wireless carriers," and therefore it was not entitled to Fourth Amendment protection.[138] The Supreme Court granted certiorari and overturned the Sixth Circuit's decision.[139]

Chief Justice Roberts began his legal analysis, echoing Justice Scalia's dissent in *King*, by recalling the reason for adopting the Fourth Amendment: colonial "general warrants" and "writs of assistance."[140] The Court acknowledged that, "[f]or much of our history, Fourth Amendment search doctrine was tied to common-law trespass and focused on whether the Government obtains information by physically intruding on a constitutionally protected area," however, a more recent precedent has established that "property rights are not the sole measure of Fourth Amendment violations."[141] This is so because "the Fourth Amendment protects people, not places," and "when an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable[,] . . . official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause."[142]

---

133 *Id*. at 2209–2210.
134 *Id*. at 2212.
135 *Id*. at 2210.
136 *Id*. at 2209.
137 *Id.* at 2212.
138 *Carpenter,* 138 S. Ct. at 2209.
139 *Id*. at 2206.
140 *Id*. at 2213 (internal quotation marks omitted).
141 *Id*. (internal quotations and citations omitted).
142 *Id*. (internal quotations and citations omitted).

While the Court acknowledged that "no single rubric definitively resolves which expectations of privacy are entitled to protection," the Fourth Amendment analysis "is informed by historical understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted."[143] Roberts then offered some basics guideposts to Fourth Amendment law, such as the "privacies of life against arbitrary power," and he explained that "the central aim of the Framers was to place obstacles in the way of a too permeating police surveillance."[144]

In accounting for how the Fourth Amendment could apply to advanced technology, the Court explained that technology has enhanced the government's capacity to encroach upon areas normally guarded from inquisitive eyes.[145] The Court explained its responsibility to "assure preservation of [the] degree of privacy against government that existed when the Fourth Amendment was adopted," but continue to adapt with technology "[b]ecause any other conclusion would leave [people] at the mercy of advancing technology."[146]

The difficulty in *Carpenter* was classifying the privacy interest maintained by the defendant, and making it fit with one line of cases defining location tracking and another line of cases concerning information offered to a third party.[147] In the first line of cases, the Court found that a person has a protectable privacy interest in the constant tracking of his location, because it is qualitatively different and more personal than other types of information.[148] In the second line of cases, the Court has held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," even if "the information is revealed on the assumption that it will be used for a limited purpose."[149]

The "third-party doctrine" traces its roots to *Miller*, mentioned earlier regarding the government's acquisition of defendant's financial information from the bank, and *Smith*, a case involving phone carriers divulging individuals' phone numbers to the government.[150] In *Carpenter*, the Court differentiated *Miller* and *Smith*, by acknowledging that "while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the *qualitatively different* category of cell-site

143 *Id*. at 2213–14.

144 *Carpenter*, 138 S. Ct. at 2214.

145 *Id*.

146 *Id*.

147 *Id*. at 2215–16.

148 *Id*. at 2215.

149 *Id*. at 2216 (citing United States v. Miller, 425 U.S. 435, 443 (1976)) (internal quotation marks omitted).

150 *See* Smith v. Maryland, 442 U.S. 735 (1979); *Miller,* 425 U.S. at 437.

records."[151] At the time of *Smith*, no one imagined a society where a phone goes wherever its owner goes and conveys information not only regarding who the owner speaks to, but also where the owner travels.[152] The Court refused to apply *Smith* and *Miller* to *Carpenter* because of the "unique nature of cell phone location records," and because a person "maintains a legitimate expectation of privacy in the record of his physical movements as captured through CLSI."[153] Therefore, the fact that the information is held by a third party "does not by itself overcome the user's claim to Fourth Amendment protection;" and "the location information obtained from Carpenter's wireless carriers was the product of a search" and required a warrant.[154]

Furthermore, the Court explained that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere[,] . . . what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[155] Society's expectation is that the government would not, and could not, monitor a person's every movement; allowing the government access to CLSI would contravene that expectation.[156] These location records "hold for many Americans the privacies of life," because a cell phone is "almost a feature of human anatomy."[157] The retrospective quality of the data also gives police access to a category of information otherwise unknowable.[158] With access to CLSI the government can "travel back in time to retrace a person's whereabouts, subject only to the retention policies of the wireless carriers," and the police "need not even need know in advance whether they want to follow a particular individual or when."[159]

On the third-party doctrine, the Court rejected the government's argument that the information was void of privacy interest solely because it was a "business record" and was in the hands of a third party.[160] There is a world of difference between the steady location tracking of an individual and his bank records or phone number.[161] The Court held the "third-party doctrine stems from the notion that an individual has a reduced expectation of privacy in information" shared with another, but "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture

151 *Carpenter*, 138 S. Ct. at 2216–17 (emphasis added).
152 *Id*.
153 *Id*. at 2217.
154 *Id*.
155 *Id*. (quoting Katz v. United States, 389 U.S. 347, 351–52 (1967)).
156 *Id*.
157 *Carpenter*, 138 S. Ct. at 2218 (internal citations and quotation marks omitted).
158 *Id*.
159 *Id*.
160 *Id*. at 2219.
161 *Id*.

entirely."[162] Because the third-party doctrine cannot be mechanically applied, the Court in *Carpenter* found there are no comparable limitations (as in *Miller* and *Smith*) on the revealing nature of CLSI (hence a finding that it is "qualitatively different").[163]

The second issue with the government's third-party doctrine argument was "voluntary exposure."[164] The Court rejected this argument because CLSI is not voluntarily "shared" as that term is understood in the third-party doctrine context.[165] Just by using a phone, "[i]n no meaningful sense does the user voluntarily assume the risk of turning over a comprehensive dossier of his physical movements."[166] With that, the Court distinguishes *Carpenter* from *Smith* and *Miller*, and finds that the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection.[167]

To be clear, the Supreme Court clarified that "its decision . . . is a narrow one," and does not "express a view on matters not before [it]."[168] It, however, reaffirms the proposition that the ultimate measure of the constitutionality of a governmental search is reasonableness, and warrantless searches are per se unreasonable (with some exceptions).[169] "This is certainly not to say that all orders compelling the production of documents will require a showing of probable cause[,] . . . only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party."[170] Thus, due to the fact that "CLSI is an entirely different species of business record" and since location information maintains a privacy interest, the Court opined that "[b]efore compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant."[171]

B. The Protection of Genetic Information

While *Carpenter* dealt with a different type of protectable private information, its reasoning, result, and guidance can inform decisions on how to better regulate the use of genetic data in crime-solving. The rationale used to address many of the issues discussed in *Carpenter* is nearly identical to this comment's proposed regulation of issues exposed by law enforcement

162 *Id*. (internal quotation marks omitted).
163 *Carpenter*, 138 S. Ct. at 2219.
164 *Id*. at 2220.
165 *Id*.
166 *Id*. at 2220 (citing Smith v. Maryland, 442 U.S. 735, 745 (1979)).
167 *Id.* at 2220.
168 *Id*.
169 *Carpenter*, 138 S. Ct. at 2221.
170 *Id*.
171 *Id*. at 2221–22.

acquiring individuals' genetic information. These two issues are: (1) whether genetic information taken from arrestees for "identification" is still valid after debunking the innocence of "junk" DNA (therefore defining it as qualitatively different or exceptional); and (2) whether the warrantless collection of DNA is reasonable where it is involuntarily abandoned, voluntarily exposed, or discovered through family ties. This issue deserves more scrutiny after Carpenter decided that certain information deserves a level of exceptionalism due to its degree of sensitivity.[172]

The Court in *King* considered the buccal swab of an arrestee a separate search from the analysis of that swab, meaning both must be reasonable under the Fourth Amendment.[173] Originally, the Court believed that only "junk DNA" was being used and that it was only used to identify the arrestee as the subject of the crime.[174] However, as the Court pointed out in *Carpenter*, and Justice Scalia identified in his dissent in *King*, certain evidence is qualitatively different. Just as *Carpenter* held that CSLI is qualitatively different than simply following someone around because tracking someone at every moment might reveal private information, collecting and then analyzing DNA from arrestees is qualitatively different than fingerprinting or photographing them because of the potential of revealing deeply personal information.

Furthermore, the Court in *King* conducted a balancing test between the interests of law enforcement officials and the interests of arrestees, and found that the physical intrusion of the arrestees was minimal, and the use of DNA was said to be harmless because it allegedly did not reveal genetic information.[175] Even though the physical buccal swab is a minimal intrusion, if the non-coding regions of DNA *do expose* personal genetic information, then the Court might need to revisit its balancing test with that in mind. The fact that experts have found personal genetic information in non-coding regions means that those areas of DNA need protection too, and as stated earlier in this comment, anonymization and aggregation of data is also not a guarantee against re-identification of a person with the data.

Where law enforcement officials collect genetic information from individuals who are not arrestees, but instead only suspects, police may acquire genetic information that is voluntarily exposed, involuntarily abandoned, or shared by family members. Each method presents problems of its own. First, genetic information that is voluntarily exposed is quite similar to that of an individual who voluntarily shares her location with a cell-service provider. Similar to individuals having their location tracked by

172 *Id*. at 2219.
173 Murphy, *supra* note 53, at 297.
174 Maryland v. King, 569 U.S. 435, 442–43 (2013).
175 *Id*.

consequence of using a phone, individuals who seek to benefit from genealogy websites' services—whether related to discovering private health information or information about one's ancestry—share the information within their DNA with these companies and allow those companies to retain that information as a consequence of the service they provide. Genetic information would also deserve protection under *Katz*, because people generally have a subjective expectation of privacy in their genetic material, and that expectation is one that society is willing to recognize since both HIPAA and GINA identify and protect such information.[176] Unlike *Miller*, where financial information was voluntarily shared with a bank, genetic information has more serious implications because of the sensitivity of the information, the information's more covert but revealing nature, and the fact that the information is more analogous to the Court's reasoning in *Carpenter*—that some types of information deserve a higher standard of protection.

Second, while law enforcement officials often treat DNA naturally left behind by suspects as "discarded," this is an inappropriate means of describing DNA. The Court in *King* defined the physical intrusion of retrieving DNA from arrestees as a separate search from the DNA analysis, so under this proposed framework even DNA that is involuntarily "abandoned" should require a second independent search warrant before it can be analyzed.[177] Where DNA is voluntarily shared with a third party, a court would look to the *Miller* Third-Party Doctrine, *Katz*'s expectation of privacy, and *Carpenter*; but where genetic information is involuntarily shed from the body, a court must consider whether or not it is fair to identify that information as "abandoned." In *Carpenter*, the Court pointed out that the cell-phone's connection to a cell tower created the location information rather than the phone actively and purposely sharing its location with the carrier.[178] In other words, the location tracking was only a product of cell usage and so it was not clear that it was voluntarily shared, but rather compulsory. DNA is also compulsorily shared and dropped in the process of everyday life, and unlike with cellphones, we cannot account for such involuntary sharing of our information. People do not expect strangers to collect and analyze their DNA as they might with discarded "trash," and so genetic information is qualitatively different than other types of expectations of privacy, and the analogy of "abandoned" DNA to trash is inappropriate.

Third, the shared aspect of DNA further complicates the analysis, because the acquisition of one individual's DNA implicates others' privacy interests, and the law should account for DNA's inherently shared nature. In

176 Ram, *supra* note 28, at 895.
177 Murphy, *supra* note 53, at 297.
178 *Carpenter*, 138 S. Ct. at 2220.

Carpenter, the Court was uneasy about the idea that the government could acquire a detailed dossier of one's every move for months, and called this information "of a unique nature" requiring a warrant.[179] Imagine if the police had access to not only the suspect's private location information, but also all of their close relatives. Surely this would have called for further protection, but the nature of technology allows for phones to be tracked individually and one phone does not necessarily implicate another. This is not the case with DNA, where one person's genetic code is shared—to varying degrees—with many people. The exposure of one person's DNA is not only private to the person who it came from, but also to family members. The inherently shared nature of DNA is extremely valuable to law enforcement because in some scenarios it may help solve an otherwise unsolvable cold case. Like the Golden State Killer, other criminals might be subsequently caught or captured using this technology, and this technology's usefulness should not be downplayed. Instead, if familial searching is something society deems appropriate, the State and Federal legislatures should draft legislation and dedicate the means to ensure it is done in accordance with the Fourth Amendment. China has revealed to the world what it looks like for a powerful police state to abuse genetic technology in order to oppress a minority, and while the Constitution protects against many misuses of government power, it is the Legislature's responsibility to regulate the Executives enforcement and investigative powers. While familial searching has its utility, genetic information is exceptionally private, immutable, and pervasive, and it must be protected as such.

V. CONCLUSION

DNA is unlike any other kind of personal information. Never before has one piece of information had the capability to reveal such detailed information about a person. From private health information, to genetic trait propensities, to relatives and ancestry, it would be irrational to give less protection to all the information within our genes than we do to all the information within our cell phones. In an age where police can acquire DNA consensually, covertly, or through familial ties, it is imperative that Fourth Amendment law, as well as State and Federal regulations, adapt to advancing technology, and act to protect Americans' privacy interests in genetic information.

179 *Id*. at 2217.