NOTE

I Just Took a DNA Test, Turns Out My Relative's a Murder Suspect: Restoring Fourth Amendment Balance to Direct-to-Consumer DNA Testing Companies

*Alexis B. Hill**

ABSTRACT

Direct-to-consumer DNA testing companies ("DTC companies") are the latest biotechnological boom. Millions of Americans in the last few years have voluntarily submitted their DNA for analysis to investigate their genetic history and locate distant relatives. These consumers, however, did not know that by submitting their DNA to DTC companies they also gave law enforcement access to their entire family's DNA. With this new expansive and comprehensive tool, police are now able to identify millions of Americans—and the number continues to grow. After the U.S. Supreme Court's latest inclination to strengthen Fourth Amendment protections of highly personal information, the Constitution likely also governs law enforcement's access to this data. But Fourth Amendment jurisprudence, federal and state legislation, and DTC company privacy policies provide inadequate protection. As a result, there is

* J.D., 2021, The George Washington University Law School; B.A., 2017, Duke University. Many thanks to Professor Kate Weisburd for not only the inspiration for this topic but also her thoughtful guidance and expertise on the Fourth Amendment jurisprudence featured in this Note, and to Professor Derek Lawlor and Brenna Fischer for their advice throughout the note-writing process. I also thank my family, who taught me curiosity, diligence, and the importance of fairness, and Michael Pronin, who has remained a steadfast sounding board and support system every step of the way. Finally, special thanks to the entire Editorial Board of *The George Washington Law Review* for their tireless work on this entire volume.

an imbalance that leaves law enforcement with unfettered access to genetic information at the expense of privacy interests.

To restore balance under the Fourth Amendment, legislators should apply the principle of informed consent to this context by requiring DTC companies to include an explicit option for consumers to opt out of law enforcement access that details the consequences of remaining in the law enforcement pool. Then, if consumers give consent, law enforcement may access this pool of DNA and lawfully use any information derived from it against suspects according to third-party consent doctrine. With valid consent to search such private information, this solution will ensure that law enforcement retains access to an important crime-solving tool without sacrificing privacy interests.

Table of Contents

Introduction

If you have not used a commercial DNA analysis kit, chances are you know someone who has. Researchers estimate that 26 million

people have submitted their DNA to direct-to-consumer DNA testing companies ("DTC companies") using these kits.[1] And this number continues to grow.[2] Researchers estimate that DNA databases can currently identify sixty percent of Americans of European ancestry from DNA.[3] In only a few years, studies project that that number will increase to ninety percent.[4] Some scientists even project that researchers will be able to identify *every* Anglo-Saxon American.[5] Soon every individual is likely to have some relational connection to a major DTC company database,[6] making these databases useful for researching family history. It also makes them useful for crime solving.

In fact, DTC companies now play a major role in crime solving. In 2018, Sacramento authorities apprehended the infamous Golden State Killer, a serial killer and rapist accused of killing twelve people and raping fifty women in the 1970s and 1980s.[7] Their secret weapon: GEDmatch, an open-source database designed to help individuals

---

1 Jason Tashea, *Genealogy Sites Give Law Enforcement a New DNA Sleuthing Tool, But the Battle Over Privacy Looms*, ABA J. (Nov. 1, 2019, 4:20 AM), http://www.abajournal.com/magazine/article/family-tree-genealogy-sites-arm-law-enforcement-with-a-new-branch-of-dna-sleuthing-but-the-battle-over-privacy-looms [https://perma.cc/7Q5Q-ASTZ].

2 Press Release, BCC Research LLC, Human Identification Market to See 14.3% Annual Growth Through 2024 (Sept. 24, 2019), https://www.bccresearch.com/pressroom/bio/human-identification-market-to-see-143-annual-growth-through-2024 [https://perma.cc/9YAA-3VTS].

3 Tashea, *supra* note 1.

4 Elizabeth Joh, *Want to See My Genes? Get a Warrant*, N.Y. TIMES (June 11, 2019), https://www.nytimes.com/2019/06/11/opinion/police-dna-warrant.html [https://perma.cc/Y6AU-S5LE].

5 Paige St. John, *DNA Genealogical Databases Are a Gold Mine for Police, but with Few Rules and Little Transparency*, L.A. TIMES (Nov. 24, 2019, 5:00 AM), https://www.latimes.com/california/story/2019-11-24/law-enforcement-dna-crime-cases-privacy [https://perma.cc/8NE6-TXGZ]. It is impossible to ignore the racial underpinnings of this statistic. While DTC company databases are designed and used primarily by individuals of European descent, *see* Joh, *supra* note 4, CODIS—the FBI's national forensic database system—comparatively houses genetic information disproportionately from Black communities. *See* Erin Murphy & Jun H. Tong, *The Racial Composition of Forensic DNA Databases*, 108 CALIF. L. REV. 1847, 1894–95 (2020). The racial implications of DTC database searches are closely tied to the debate about universal DNA databases. *See id.* at 1909 (summarizing the debate about race and universal DNA databases for police access). Though the racial implications of DTC searches are certainly an important consideration in the context of law enforcement, particularly for eliminating racial bias in policing, it is beyond the scope of this Note.

6 *Cf.* Kashmir Hill & Heather Murphy, *Your DNA Profile is Private? A Florida Judge Just Said Otherwise*, N.Y. TIMES (Dec. 30, 2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html?auth=login-email&login=email [https://perma.cc/RQ9N-BYDV].

7 Keith Allen, Jason Hanna & Cheri Mossburg, *Police Used Free Genealogy Database to Track Golden State Killer Suspect, Investigator Says*, CNN (Apr. 27, 2018, 2:25 PM), https://www.cnn.com/2018/04/26/us/golden-state-killer-dna-report/index.html [https://perma.cc/P8AQ-C2F7].

find genetic relatives by contributing information from other DTC companies.[8] After the success of the Golden State Killer case, police nationwide have solved dozens of other cold cases using DTC company databases.[9] Police are also turning to these databases to solve less serious and more recent crimes.[10] In 2019, police even saw their first DTC database-driven conviction.[11]

In the wake of this phenomenon, however, consumers are growing concerned about their privacy, fearing the possibility of an impending surveillance state.[12] With the exception of an interim policy issued by the Department of Justice ("DOJ") in late 2019,[13] DTC company database searches operate in the Wild West, with very little oversight over police behavior.[14] Moreover, current Fourth Amendment jurisprudence, federal and state legislation, and internal privacy policies do little to help protect consumers' privacy.[15] Given that DTC companies will soon be able to identify the vast majority of the American population, it will not be long before police have the unfettered

---

8 George M. Dery III, *Can a Distant Relative Allow the Government Access to Your DNA?*, 10 HASTINGS SCI. & TECH. L.J. 103, 112 (2019).

9 *See, e.g.*, Robert Gearty, *Washington State Teen's Cold Case Murder Cracked After Nearly Three Decades*, FOX NEWS (Oct. 4, 2019), https://www.foxnews.com/us/washington-state-teens-cold-case-murder [https://perma.cc/R7A3-8S24]; Taylor Stevens, *Clearfield Police Arrest Alleged Serial Rapist with the Use of a DNA Database*, SALT LAKE TRIB. (Sept. 26, 2019), https://www.sltrib.com/news/2019/09/26/clearfield-police-arrest/ [https://perma.cc/AW5R-28UG]; Tashea, *supra* note 1.

10 *See* Hill & Murphy, *supra* note 6. For example, in Clearfield, Utah, Mark Douglas Burns was charged with multiple counts of aggravated sexual assault, aggravated kidnapping, aggravated burglary, and aggravated robbery all based on an investigation through GEDmatch. Stevens, *supra* note 9.

11 *SeaTac Man Convicted of 1987 Murders of Canadian Couple After DNA Evidence Linked Him to Case*, SEATTLE TIMES (June 28, 2019, 3:58 PM), https://www.seattletimes.com/seattle-news/crime/seatac-man-convicted-of-1987-murders-of-canadian-couple-after-dna-evidence-linked-him-to-case/ [https://perma.cc/469V-C4SD] (reporting conviction of a man from Washington that arose out of Snohomish County detective using GEDmatch to locate Talbott based on DNA information from two unrelated second cases).

12 *See, e.g.*, Jon Schuppe, *'They Lied to Us': Mom Says Police Deceived Her to Get Her DNA and Charge Her Son with Murder*, NBC NEWS (Feb. 22, 2020, 4:00 PM), https://www.nbcnews.com/news/us-news/they-lied-us-mom-says-police-deceived-her-get-her-n1140696 [https://perma.cc/65HS-D3N4] (reporting that parents were outraged that police had used their DNA to build a case against their son with genetic analysis).

13 U.S. DEP'T OF JUST., INTERIM POLICY: FORENSIC GENETIC GENEALOGICAL DNA ANALYSIS AND SEARCHING 1–2 (2019) [hereinafter DOJ INTERIM POLICY], https://www.justice.gov/olp/page/file/1204386/download [https://perma.cc/6U9M-22J7].

14 St. John, *supra* note 5.

15 *See infra* Sections I.B–.D.

ability to investigate millions of individuals' personal biological data without their knowledge.[16]

The Fourth Amendment[17] should protect individuals' privacy interests in their DNA from undue invasion by law enforcement.[18] The Fourth Amendment generally seeks to balance law enforcement's interests in crime solving with the public's interest in maintaining privacy.[19] In light of a recent U.S. Supreme Court ruling that suggests that the Court is inclined to protect information shared with third parties if it is highly personal and deeply revealing,[20] it is likely that DNA—highly personal and deeply revealing biological information—is governed by the Fourth Amendment, and therefore, DTC company database searches should reflect this balance.[21] Today's status of police searches of commercial DNA databases, however, is tilted significantly in favor of law enforcement, with little to no protections for personal privacy.[22]

This Note provides a solution to restore the balance. Federal and state legislators should import informed consent principles from the medical context into this Fourth Amendment inquiry by requiring DTC companies to include an explicit option at the outset for consumers who provide DNA to DTC companies[23] to remove their DNA information from law enforcement access. Specifically, this option should notify consumers of the ramifications of their choice before asking if they would like to remain in this pool. Consumers will encounter a separate webpage when signing up for the service that informs a consumer that her DNA may be used against herself or her close and distant family in a criminal investigation, but that she can withdraw from the law enforcement pool at any time after subscription. In doing so, legislators can ensure that police only access the profiles of those who have knowingly agreed to such surveillance, leaving the public who want to protect their personal biological data

16 *See* St. John, *supra* note 5.

17 U.S. CONST. amend. IV.

18 *See* Katz v. United States, 389 U.S. 347, 351 (1967) (holding that the Fourth Amendment protects an individual's reasonable expectation of privacy).

19 *See* Maryland v. King, 569 U.S. 435, 448 (2013) (explaining that a court must weigh "'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy'" (alteration in original) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))).

20 *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).

21 *See infra* Section I.B.

22 *See infra* Sections I.B–.D.

23 Throughout, this Note refers to individuals who purchase the DNA testing kits and provide their DNA to DTC companies as "consumers."

out of reach while ensuring that law enforcement still have access to this helpful tool. Law enforcement may then access this limited pool of DNA to investigate a suspect because under third-party consent principles, a suspect and consumer share common authority over the shared portion of their DNA, thus allowing a consumer to consent to a DNA search against the suspect. By adopting this two-layer solution combining and applying informed consent and third-party consent principles, legislators can ensure they are balancing privacy interests against law enforcement interests with legal doctrines that appropriately capture DNA's shared and biological nature.

Part I summarizes the legal issues surrounding DNA and law enforcement access to consumers' DNA. Part I explains that DNA is highly personal in nature and law enforcement intrudes more deeply into this personal information when they use DTC companies than when they use government-sponsored DNA analysis such as CODIS. Part I then continues to discuss how Fourth Amendment jurisprudence, federal and state legislation, and internal privacy policies do little to restrain this greater intrusion into such private data, leading to an imbalance under the Fourth Amendment that favors law enforcement. Part II addresses how consent can easily remedy Fourth Amendment imbalances like this one and examines different forms of legal consent. Part II then contrasts the flexible standards of consent in the Fourth Amendment context and the digital sphere with the heightened standard in the medical context—informed consent—noting that this heightened standard serves as better protection of bodily privacy interests. Part III advocates that federal and state legislators apply informed consent requirements by obligating DTC companies to notify consumers of the consequences associated with remaining in a pool that law enforcement can access before soliciting the consumers' affirmative consent. Law enforcement can then use this consent against suspects pursuant to third-party consent because consumers and suspects have common authority to consent to searches of shared portions of their DNA against the other. Part III concludes by explaining the logical justifications for this solution and addresses counterarguments related to contracts of adhesion, scope, and sufficient common authority.

I. DNA AND THE LAW

Deoxyribonucleic acid ("DNA") reveals a host of very personal genetic information.[24] Simultaneously, DNA testing has the "unparalleled ability . . . to identify the guilty . . . [and] the potential to significantly improve both the criminal justice system and police investigative practices."[25] As a result, police have every incentive to tap into this technology.[26] Police intrusions into such private information, however, pose particular legal questions, especially when police access private information through DTC company databases.[27] This Part details how law enforcement has taken advantage of the wealth of information that DNA holds, and how current Fourth Amendment jurisprudence, state and federal legislation, and internal privacy policies fail to protect against these privacy intrusions.

A. Crime Solving with DNA

DNA contains a wealth of information about a person, "hold[ing] the secret to such personal details as one's Neanderthal ancestry, the potential for afflictions with rare diseases, and paternity."[28] Each individual also shares significant portions of their DNA with other closely related individuals in their family,[29] making DNA a key to information about other people in her family as well as herself.

Federal and state governments have capitalized on DNA by establishing national and state databases to collect samples from any individual who interacts with law enforcement through arrest, charges, or conviction.[30] The national effort to support forensic DNA databases, commonly referred to as the Combined DNA Index System ("CODIS"), uses software to analyze DNA for full and partial

---

24 *See* Maggie Fox, *What You're Giving Away with Those Home DNA Tests: It's the Most Valuable Thing You Own*, NBC NEWS (Nov. 29, 2017, 6:46 AM), https://www.nbcnews.com/health/health-news/what-you-re-giving-away-those-home-dna-tests-n824776 [https://perma.cc/S7JE-XWXN].

25 Dist. Att'y's Off. for the Third Jud. Dist. v. Osborne, 557 U.S. 52, 55 (2009).

26 *See* Claire Abrahamson, Note, *Guilt by Genetic Association: The Fourth Amendment and the Search of Private Genetic Databases by Law Enforcement*, 87 FORDHAM L. REV. 2539, 2546 (2019) (discussing the advantages and capabilities of using DNA testing technology in law enforcement).

27 Natalie Ram, Christi J. Guerrini & Amy L. McGuire, *Genealogy Databases and the Future of Criminal Investigation*, 360 SCI. 1078, 1078 (2018).

28 Dery, *supra* note 8, at 107.

29 Christine Guest, Comment, *DNA and Law Enforcement: How the Use of Open Source DNA Databases Violates Privacy Rights*, 68 AM. U. L. REV. 1015, 1022 (2019).

30 *See* Abrahamson, *supra* note 26, at 2546.

matches in an effort to identify culprits of other crimes.[31] CODIS compares between thirteen and twenty locations, called single-tandem repeat ("STR") markers, on regions of noncoding DNA to find a match between a sample obtained from a crime scene ("forensic sample") and one or more reference samples.[32] Noncoding DNA searches are inherently limited because they only reveal identity and do not reveal genetic traits.[33] The federal government does not explicitly authorize familial DNA testing, but police may conduct searches to return a *partial* match that indicates a biological relation by comparing suspect DNA profiles with offender DNA profiles.[34] As of January 2021, the National DNA Index ("NDIS") contained over 14 million DNA profiles of criminal offenders, over 4 million arrestees, and over 1 million forensic samples, giving law enforcement an immense and powerful tool to search for matches.[35]

Even with access to a tool as advantageous as CODIS, law enforcement has sought an alternative method of ferreting out crimes with DNA: DTC company databases. In exchange for saliva and a fee, consumers can send their DNA to DTC companies like 23andMe or FamilyTreeDNA, which will analyze their DNA and report back personal information such as distant biological relatives, genetic predispositions to certain health issues, or ancestry.[36] Law enforcement accesses a DTC company database, either by anonymously submitting forensic samples to the company[37] or by obtaining a warrant to access the company's database,[38] in the hopes of discovering full or partial matches to DNA that will generate a suspect unknown to CODIS.[39]

---

31 *See id.*

32 DOJ INTERIM POLICY, *supra* note 13, at 2.

33 *See* Abrahamson, *supra* note 26, at 2547.

34 Guest, *supra* note 29, at 1027–28.

35 *CODIS - NDIS Statistics*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/ndis-statistics [https://perma.cc/JP5D-XZYV]. As of January 2021, CODIS has aided law enforcement in over half a million investigations, reflecting the power of DNA in helping to solve crimes. *Id.*

36 *See* Amy Dockser Marcus, *What Consumers Should Know About Commercial DNA Testing*, WALL ST. J. (Sept. 14, 2018, 3:13 PM), https://www.wsj.com/articles/what-consumers-should-know-about-commercial-dna-testing-1536952428 [https://perma.cc/SA5K-4QQD].

37 *See* Heather Murphy, *What You're Unwrapping When You Get a DNA Test for Christmas*, N.Y. TIMES (Dec. 23, 2019), https://www.nytimes.com/2019/12/22/science/dna-testing-kit-present.html [https://perma.cc/GBL7-9Q8M].

38 Hill & Murphy, *supra* note 6.

39 DTC testing is also a leading tool in exonerating wrongfully convicted individuals. *See* Mia Armstrong, *In an Apparent First, Genetic Genealogy Aids a Wrongful Conviction Case*, MARSHALL PROJECT (July 17, 2019, 4:45 PM), https://www.themarshallproject.org/2019/07/16/in-an-apparent-first-genetic-genealogy-aids-a-wrongful-conviction-case [https://perma.cc/3AC9-

As searches of DTC company databases increased, DOJ released a set of guidelines for how to properly conduct DTC company database searches in November 2019.[40] In doing so, DOJ set several limits on when and how law enforcement can use these methods,[41] effectively designating the use of DTC company databases as a last resort.[42]

Even with the presence of DOJ guidelines, there are still serious privacy implications. DTC companies' analysis of DNA differs from CODIS in two ways. First, DTC companies analyze thousands of DNA datapoints, dwarfing the forty datapoints analyzed in CODIS.[43] Second, unlike STR markers in CODIS, which only reveal identity, the single nucleotide polymorphisms ("SNPs")[44] that DTC companies analyze can reveal information about ancestry, genetic characteristics, race, and medical history.[45] DTC companies consequently analyze a much greater portion of DNA for personal information beyond mere identification, surpassing the invasion of privacy that CODIS presents.

DTC databases are also expected to increase in the years to come. Commercial DNA testing boomed in the last few years, rapidly expanding DTC companies' collections of DNA.[46] One study found that approximately sixty percent of those of European descent could be identified through DTC company databases.[47] In 2017 and 2018

5GJ8]; Catherine Arcabascio, *A Genetic Surveillance State: Are We One Buccal Swab Away From A Total Loss of Genetic Privacy?*, 63 How. L.J. 117, 143 (2020).

40 DOJ Interim Policy, *supra* note 13.

41 First, law enforcement can only analyze DNA obtained from crime scenes of unsolved violent crimes, sexual offenses, or other crimes threatening public safety. *Id.* at 4. Second, before submitting DNA for analysis, an investigative agency must have exhausted all other reasonable leads to solve the case and have the case reviewed and deemed suitable for uploading to a DTC database by both a prosecutor and designated official at a CODIS lab. *Id.* at 5–6. Third, law enforcement can only use any matches generated by the DTC database as an investigative lead after which they should use traditional genealogy research and investigative work to determine the true nature of any genetic relatives. *Id.* at 4.

42 There is room for argument that extending the use to offenses that are a threat to public safety gives law enforcement discretion to extend DNA database searches to a vast array of crimes. Jesse Schwab, *New DOJ Policy Gives Genealogy Website Users Weak Privacy Protections from Law Enforcement*, Harv. C.R.-C.L. L. Rev. Amicus Blog (Oct. 3, 2019), https://harvardcrcl.org/new-doj-policy-gives-genealogy-website-users-weak-privacy-protections-from-law-enforcement/ [https://perma.cc/G84D-XSRJ].

43 Guest, *supra* note 29, at 1030; Natalie Ram, *Genetic Privacy After* Carpenter, 105 Va. L. Rev. 1357, 1377–79 (2019).

44 SNPs are variations in DNA sequences at particular locations that "generate biological variation between people by causing differences" in protein generation in genes that influence a variety of genetic traits. *What Are SNPs?*, 23andMe, https://www.23andme.com/gen101/snps/ [https://perma.cc/8JZH-L8RX].

45 Guest, *supra* note 29, at 1023–24.

46 *See* Abrahamson, *supra* note 26, at 2548.

47 Guest, *supra* note 29, at 1034.

alone, 7.8 million individuals submitted their DNA to DTC companies.[48] Due to a growing public interest in genealogy, the DTC market will likely grow at a compound annual rate of 14.3% through 2024, resulting in a $83.9 billion industry.[49] With this growth, it is likely police will soon have access to a vast majority of Americans' DNA as long as they have access to DTC company databases.[50]

B. Fourth Amendment Protections of DNA

As law enforcement increasingly uses DTC companies to implicate the public, courts will have to address the constitutional limits of these searches. The Fourth Amendment[51] governs the constitutional limits of police action by protecting individual privacy from undue government invasion.[52] The Fourth Amendment attempts to balance the interests of law enforcement with an individual's interest in protecting her privacy.[53] This balancing, however, only arises if some police activity falls under the purview of the Fourth Amendment in the first place—that is, if the individual has a reasonable expectation of privacy in the item searched.[54] Under the *Katz* test,[55] the Fourth Amendment requires an individual to have both "an actual (subjective) expectation of privacy" in some item and an expectation of privacy "that society is prepared to recognize as 'reasonable.'"[56] The U.S. Supreme Court has yet to decide whether police analysis of consum-

48 Abrahamson, *supra* note 26, at 2548.

49 Press Release, BCC Research LLC, *supra* note 2.

50 *See* Guest, *supra* note 29, at 1035.

51 U.S. CONST. amend. IV.

52 Katz v. United States, 389 U.S. 347, 350 (1967) (explaining that the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion").

53 *See* Maryland v. King, 569 U.S. 435, 448 (2013) (explaining that a court must weigh "'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy'" (alteration in original) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))).

54 *See Katz*, 389 U.S. at 351–52 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." (citations omitted)).

55 This test was derived from Justice Harlan's concurrence in *Katz*. *See* 389 U.S. at 361 (Harlan, J., concurring). The *Katz* test has been subsequently cited as the appropriate inquiry for whether Fourth Amendment protection applies. *See, e.g.*, Byrd v. United States, 138 S. Ct. 1518, 1526 (2018) ("[T]he test most often associated with legitimate expectations of privacy . . . was derived from the second Justice Harlan's concurrence in *Katz v. United States* . . . .").

56 *Katz*, 389 U.S. at 361 (Harlan, J., concurring). ("[T]here is a twofold requirement [to determine whether the Fourth Amendment protects some activity], 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.'").

ers' DNA is regulated by the Fourth Amendment.[57] Nevertheless, because the Court concluded that analysis of biological samples falls under the Fourth Amendment, and because the Court recently indicated a limitation on the third-party doctrine,[58] it is likely that police access to these DTC company databases is subject to the Fourth Amendment.

1. Chemical Analyses

Chemical analyses of biological samples fall under the Fourth Amendment's protection as established by the Supreme Court. In *Skinner v. Railway Labor Executives' Ass'n*,[59] the Court held that chemical analyses of urine are subject to the Fourth Amendment because they "can reveal a host of private medical facts about an [individual]."[60] The Court reaffirmed *Skinner* in *Ferguson v. City of Charleston*,[61] holding that urine tests conducted by hospital staff and sent to the police were "indisputably searches within the meaning of the Fourth Amendment."[62] Closer in kind to DNA, the Court held that blood tests are Fourth Amendment searches because they constitute intrusions into the human body.[63] Indeed, the Court recently suggested that this type of analysis was so personal that mere implied-consent laws were not enough to render the search reasonable.[64]

In *Maryland v. King*,[65] the Court relied on this chemical analysis precedent in finding that a buccal swab for DNA and subsequent

---

57 *See* Guest, *supra* note 29, at 1038.

58 *See infra* Section I.B.2.

59 489 U.S. 602 (1989).

60 *Id.* at 616–17.

61 532 U.S. 67 (2001).

62 *Id.* at 76.

63 *See* Mitchell v. Wisconsin, 139 S. Ct. 2525, 2534 (2019) ("A blood draw is a search of the person . . . ."); Schmerber v. California, 384 U.S. 757, 767 (1966) (holding that blood tests "plainly constitute searches of 'persons'").

64 *See Mitchell*, 139 S. Ct. at 2533 ("[O]ur decisions have not rested on the idea that these laws do what their popular name might seem to suggest—that is, create actual consent to all the searches they authorize."). The Court did hold in *Mitchell* that blood draws in driving under the influence situations are almost per se reasonable under the exigent circumstances exception for the warrant requirement. *Id.* at 2531 (discussing that blood draws when drivers are unconscious and unable to give consent qualifies as an exigent circumstance, and are thus "almost always permi[ssible]"). Exigency, however, cannot apply to law enforcement access of DTC databases because there is no reason to believe that destruction of the DNA evidence is imminent given that it is stored long term. *See* Missouri v. McNeely, 569 U.S. 141, 148–49 (2013) (explaining that law enforcement can search without a warrant if they have a compelling need to conduct the search and no time to secure a warrant).

65 569 U.S. 435 (2013).

CODIS analysis was a search under the Fourth Amendment.[66] Even though the Court ultimately found the search reasonable, the Court noted the "revealing power of . . . DNA."[67] The only justifications for the reasonableness of these searches[68] were that the government had an overwhelming interest in safe and accurate identification of custodial arrestees,[69] the analyses were conducted purely for identification purposes,[70] and the overall expectation of privacy in arrestees was already diminished.[71]

Applying these doctrines, it is likely that courts will find DTC company database searches subject to the Fourth Amendment. Just like blood draws and urine analyses, analysis of DNA data is highly personal and invasive, which was acknowledged implicitly in *King*.[72] The reasons that saved the searches in *King* also do not apply to a database filled with DNA information of ordinary members of the public.[73] In a local jail, police need to accurately identify arrestees to ensure the safety of inmates, but in the broader public, there is no similar safety justification for searching through individuals' DNA.[74] Unlike arrestees, consumers are not in custody or detention and therefore do not already have a diminished expectation of privacy.[75] And unlike the analysis that is limited to identification used in CODIS, DTC company analysis inspects a much deeper and broader scope of genetic information.[76] *King* therefore strongly suggests that law enforcement investigations into the DNA of non-inmates intrude on consumers' reasonable expectation of privacy.[77]

---

66 *Id.* at 446.

67 *Id.* at 459.

68 *Id.* at 446.

69 *Id.* at 449.

70 *Id.* at 464.

71 *Id.* at 462.

72 *See id.* at 446.

73 Ram, *supra* note 43, at 1385.

74 *Id.* at 1386; *cf. King*, 569 U.S. at 449 (finding the government's interest in ensuring the safety of their inmates through an accurate booking procedure was compelling).

75 Ram, *supra* note 43, at 1386; *cf. King*, 569 U.S. at 462 (explaining that because arrestees are in custody or detention, their privacy interests in their DNA are already diminished despite the revealing nature of DNA).

76 *See supra* notes 43–45 and accompanying text; *cf. King*, 569 U.S. at 464 (explaining that CODIS's limitations to identification indicated that the privacy intrusion into this genetic information was minimal).

77 Ram, *supra* note 43, at 1386.

2. *Third-Party Doctrine*

Even if DNA information implicates privacy rights, searches of DTC databases may be exempt from the Fourth Amendment under the third-party doctrine because consumers willingly reveal their DNA to these third-party companies. The Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"[78] because when individuals disclose information to a third party, they assume the risk that the information will be turned over to the police.[79] Third-party doctrine applies "even if the information is revealed on the assumption that it will be used only for a limited purpose."[80]

As established by the Court's recent decision in *Carpenter v. United States*,[81] however, depending on the "nature of the particular [information] sought,"[82] disclosing information to third parties does not automatically "surrender all Fourth Amendment protection."[83] If the information sought is comprehensive, deeply revealing, and involuntarily conveyed, then it may retain Fourth Amendment protections.[84] For example, the *Carpenter* Court found that location information obtained from smartphones connecting to cell sites and generating a time-stamped record[85] was protected by the Fourth Amendment because the cell sites are found all over the country, thereby creating an all-encompassing record of each minute change in the location of those carrying smartphones, an almost involuntary component of life in the modern age.[86] *Carpenter* represents the Court's inclination to take a step back from the all-encompassing third-party doctrine in favor of protecting large swaths of digital information, a positive sign for the fate of consumer privacy interests implicated by DTC company database searches.

In light of the *Carpenter* decision, the comprehensive, deeply revealing, and involuntarily conveyed nature of DNA arguably gives DNA information the same Fourth Amendment protection. Justice Gorsuch recognized this conclusion when dissenting in the *Carpenter* judgment, noting that permitting the government to acquire genetic

78 Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

79 *See* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

80 United States v. Miller, 425 U.S. 435, 443 (1976).

81 138 S. Ct. 2206.

82 *Id.* at 2219 (quoting *Miller*, 425 U.S. at 442).

83 *Id.* at 2217.

84 *See id.* at 2219–20; Abrahamson, *supra* note 26, at 2558–59.

85 *Carpenter*, 138 S. Ct. at 2211–12.

86 *Id.* at 2219–20.

information from DTC company databases without a warrant or probable cause "strikes most lawyers and judges today—[him] included—as pretty unlikely."[87] Thus, even though DNA is disclosed to a third party (in this context, DTC companies), *Carpenter* suggests that DNA information is likely a search under the Fourth Amendment, much like cell-site location information.[88]

Whether the Fourth Amendment governs a particular government action, however, is only the first inquiry in typical Fourth Amendment analyses—the next inquiry is whether the search is reasonable, meaning whether there was a warrant for the search or a valid exception exempting the need for a warrant.[89] *King* and *Carpenter* offer little instruction on how to proceed with DTC company database searches once they are found to fall under the Fourth Amendment as there is no guidance as to exactly when it may be reasonable for police to access this personal information. The lack of guidance leaves those whose privacy interests are intruded upon without adequate protection. This inadequate protection is also exacerbated by the fact that whether the Fourth Amendment protects these interests is concededly still unresolved. A clearer and more effective solution is necessary to adequately fill this gap.

C. Attempts to Regulate Individual DNA Information

If the Fourth Amendment is deficient, Congress and state legislators can step in with additional safeguards by directly regulating the activities that implicate the Fourth Amendment.[90] The Fourth Amendment represents a "floor" in protecting privacy interests, which legislatures can surpass.[91] This has become commonplace as modern technology advances.[92] Current law does not cover DTC companies,[93]

---

87 *Id.* at 2262 (Gorsuch, J., dissenting).

88 *E.g.*, Abrahamson, *supra* note 26, at 2539; Dery, *supra* note 8, at 103; Guest, *supra* note 29; Ram, *supra* note 43, at 1386–88.

89 *See* Mitchell v. Wisconsin, 139 S. Ct. 2525, 2534 (2019) ("The Fourth Amendment guards the 'right of the people to be secure in their persons . . . against unreasonable searches' and provides that 'no Warrants shall issue, but upon probable cause.'" (alteration in original) (quoting U.S. CONST. amend. IV)).

90 *See* Louis Fisher, *Congress and the Fourth Amendment*, 21 GA. L. REV. 107, 107 (1986) ("Congress helps fill important gaps in the law on search and seizure . . . and intervenes to safeguard [F]ourth [A]mendment interests left unprotected by court decisions.").

91 *See* Marc L. Miller & Ronald F. Wright, *Leaky Floors: State Law Below Federal Constitutional Limits*, 50 ARIZ. L. REV. 227, 228 (2008) ("One of the most widely accepted notions in American constitutional law is that the federal Constitution and interpretations of that Constitution by the Supreme Court of the United States set a 'floor' for personal liberties. State courts and state legislatures cannot properly go below the federal floor.").

92 *See* Amanda Regan, Note, *Dumping the Probable Cause Requirement: Why the Supreme*

however, leaving individuals who submit their DNA to these companies without any enforceable privacy protections.

Over thirty states have enacted laws designed to protect genetic information in some way.[94] Alaska's Genetic Privacy statute,[95] for example, requires written consent before collection, analysis, or retention of a DNA sample and disclosure of DNA analysis results.[96] Minnesota also prohibits collection of genetic information by a government entity without written informed consent of the consumer.[97] More recently, Illinois passed legislation that specifically prohibited DTC companies from sharing genetic information with a health or life insurance provider without written consent from the consumer.[98] But all of these statutes, as is the case with most state legislation protecting genetic information, explicitly do not protect against law enforcement use of DTC companies' data.[99]

The same is true for the federal regulatory scheme. In terms of agency regulations, neither the U.S. Food and Drug Administration ("FDA") nor the Federal Trade Commission ("FTC") have elected to regulate privacy issues when it comes to DTC companies.[100] One piece of legislation that might cover this area is the Health Insurance Porta-

---

Court Should Decide Probable Cause Is Not Necessary for Cell Tower Dumps, 43 HOFSTRA L. REV. 1189, 1195 (2015) ("As technology advances, Congress has passed some legislation to supply greater protections beyond those extended by the Fourth Amendment.").

93 Memorandum from Nathan Hopkins, Legislative Analyst, Minnesota House of Representatives, to Members of the Minnesota Legis. Comm'n on Data Pracs. & Pers. Data Priv. 6 (Nov. 15, 2018), https://www.lcc.leg.mn/lcdp/meetings/11162018/Consumer-Privacy-and-Genetic-Testing-memo-11-15-18.pdf [https://perma.cc/J4CR-5HN9].

94 Ram, *supra* note 43, at 1382.

95 ALASKA STAT. § 18.13.010 (2019).

96 *Id.* § 18.13.010(a)(1).

97 MINN. STAT. § 13.386, subdiv. 3(a)(1) (2019).

98 410 ILL. COMP. STAT. 513/20(e) (2020).

99 *See* ALASKA STAT. § 18.13.010(b)(2) (providing a carveout "for a law enforcement purpose, including the identification of perpetrators and the investigation of crimes"); 410 ILL. COMP. STAT. 513/20(e) (only prohibiting disclosure to "any health or life insurance company"); MINN. STAT. § 13.386 (limited to data held by government entities, not third parties); *see also, e.g.*, OR. REV. STAT. § 192.535 (2019) (prohibiting obtention of genetic information without informed consent except "for the purpose of establishing the identity of a person in the course of an investigation conducted by a law enforcement agency"); N.J. STAT. ANN. § 10:5-45(a)(1) (West 2020) (exempting from informed consent requirements genetic information obtained "for the purposes of establishing the identity of a person in the course of a criminal investigation or prosecution").

100 The FDA and the FTC do regulate DTC companies but such regulations relate to test accuracy and marketing, not privacy. *See Direct-to-Consumer Tests*, U.S. FOOD & DRUG ADMIN. (Dec. 20, 2019), https://www.fda.gov/medical-devices/vitro-diagnostics/direct-consumer-tests [https://perma.cc/6XY7-R8Z9]; CONSUMER REPORTS, DIRECT-TO-CONSUMER GENETIC TESTING: THE LAW MUST PROTECT CONSUMERS' GENETIC PRIVACY 11–13 (2020), https://advo-

bility and Accountability Act of 1996 ("HIPAA").[101] HIPAA protects the use and disclosure of individually identifiable health information, such as genetic information, by organizations subject to the rule.[102] Any entity covered by the statute may not use or disclose medical information without written consent.[103] Covered entities, however, do not include DTC companies.[104] HIPAA only extends the definition of "covered entities" to health care professionals, health plans (e.g., health insurance companies), and health care clearinghouses.[105] In fact, HIPAA provides an explicit exception for use by law enforcement to use otherwise protected medical information in order to identify or locate a suspect or search for evidence of a crime.[106] The same issue occurs in the Genetic Information Nondiscrimination Act ("GINA"),[107] which builds on HIPAA protections by prohibiting covered entities from collecting genetic information.[108] Although GINA creates additional genetic safeguards, "it fails to address concerns of surreptitious collection and testing of DNA" outside of these covered entities.[109] Law enforcement access to DTC companies, therefore, falls outside of the regulatory scope of both HIPAA and GINA, leaving DTC companies largely unregulated at the federal level as well as the state level.[110]

D. The Problem with DTC Databases

Although the U.S. Supreme Court, legislators, and legal scholars are beginning to address privacy dilemmas with government DNA

---

cacy.consumerreports.org/wp-content/uploads/2020/07/DTC-Genetic-Testing-White-Paper.pdf [https://perma.cc/2U92-VASE].

101 Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

102 *See* U.S. DEP'T OF HEALTH & HUM. SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 1 (2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf [https://perma.cc/7SDS-8U7M].

103 *Id.* at 4.

104 Colin McFerrin, Comment, *DNA, Genetic Material, and a Look at Property Rights: Why You May Be Your Brother's Keeper*, 19 TEX. WESLEYAN L. REV. 967, 983 (2013).

105 *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 102, at 2.

106 *See id.* at 7.

107 Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.). GINA "prohibits discrimination in group health plan coverage based on genetic information." U.S. DEP'T OF LAB., THE GENETIC INFORMATION NONDISCRIMINATION ACT (GINA) FACT SHEET 1, https://www.dol.gov/sites/dolgov/files/EBSA/about-ebsa/our-activities/resource-center/fact-sheets/gina.pdf [https://perma.cc/UMW2-DP7U].

108 U.S. DEP'T OF LAB., *supra* note 107, at 1.

109 McFerrin, *supra* note 104, at 984–85.

110 *See id.* at 982–85.

analysis, there are almost no regulations or legal restraints on government use of DTC companies for DNA evidence.[111] Even a Congressional bill proposed in 2019 to create more protections for genetic information failed to adequately address the use by law enforcement.[112] This deficiency leaves the heightened privacy interest in DNA information largely unprotected from potentially almost unlimited, and perhaps unreasonable, law enforcement access.

There are also no clear internal constraints on the DTC companies to ensure privacy interests are well protected. Although all DTC companies have privacy policies specifically targeting law enforcement searches, they vary among companies. 23andMe states that it "use[s] all practical legal and administrative resources to resist requests from law enforcement, . . . [it] do[es] not share customer data with any public databases, or with entities that may increase the risk of law enforcement access," and agreeing to its terms of services means that individuals agree not to contact other customers or use the data for forensic purposes.[113]

FamilyTreeDNA, a company that was revealed in 2019 to have been secretly working with the FBI in cold case investigations,[114] has since adopted an option for consumers to remove law enforcement access,[115] but also states that it "takes every action possible to protect user privacy" and that before granting any request for access from law enforcement, it will "notify users" and supply them with copies of those requests, unless "doing so would be considered counterproductive and . . . [it is] not legally permitted to do so."[116] GEDmatch, the predominant resource used in law enforcement searches, originally al-

111 Antony Barone Kolenc, *"23 and Plea": Limiting Police Use of Genealogy Sites After* Carpenter v. United States, 122 W. VA. L. REV. 53, 103 (2019); *see supra* Section II.C.

112 *See* Genetic Information Privacy Act of 2019, H.R. 2155, 116th Cong. (2019) (prohibiting genetic testing services from disclosing personally identifiable genetic information to third parties without express informed consent but failing to adequately regulate disclosure requirements as they pertain to law enforcement).

113 *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide/ [https://perma.cc/Q3WN-2QV4]. Ancestry.com states that it "does not voluntarily cooperate with law enforcement[,] . . . require[s] all government agencies seeking access to Ancestry customers' data to follow valid legal process[,] and do[es] not allow law enforcement to use Ancestry's services to investigate crimes or to identify human remains." *Ancestry Guide for Law Enforcement*, ANCESTRY, https://www.ancestry.com/cs/legal/lawenforcement [https://perma.cc/GZ84-WR2U]. It is questionable, however, how much weight this promise will hold if faced with a valid court order. *See* Hill & Murphy, *supra* note 6.

114 Ram, *supra* note 43, at 1363.

115 *Id.*

116 *FamilyTreeDNA Law Enforcement Guide*, FAMILYTREEDNA, https://www.familytreedna.com/legal/law-enforcement-guide (last visited Mar. 16, 2021).

lowed law enforcement unfettered access.[117] But, in May 2019, GEDmatch updated its policies, requiring that existing users would have to opt in before their DNA kits would become subject to law enforcement use.[118] New genetic profiles, however, are "opted-in by default."[119]

Some companies openly encourage law enforcement access. For example, the DNA Doe Project actively uses databases to identify unidentified bodies.[120] Even FamilyTreeDNA, which maintains that it "takes every action possible to protect user privacy" against law enforcement,[121] was revealed to have run an advertisement starring a relative of a kidnapping victim who encouraged customers to upload profiles to help solve crimes.[122] More recently, even GEDmatch appears to be at risk of unfettered law enforcement use, as it was recently acquired by forensic genomics company Verogen, Inc.[123]

Under these varying privacy policies and conflicting behaviors, it is uncertain exactly how private a consumer's DNA remains once she gives it to a DTC company. This poses a particular problem given the broad scope of privacy implications at stake. Not only are particular individuals who are already subject to the criminal justice system subject to these intrusions, as was the case in *King*,[124] but now most of the American population is subject to the same scrutiny, sometimes to the detriment of criminal suspects.[125] As DTC companies grow and law enforcement access to them remains unchecked, the country will approach the "genetic panopticon" Justice Scalia warned of in *King*.[126] The evolution creates an imbalance in the field of government use of DTC companies that overtly favors police's unrestricted access to the

117 *See* Ram, *supra* note 43, at 1362.

118 *See* Ram, *supra* note 43, at 1362–63.

119 *Id.*

120 *See* Sarah Zhang, *The Messy Consequences of the Golden State Killer Case*, ATLANTIC (Oct. 1, 2019) https://www.theatlantic.com/science/archive/2019/10/genetic-genealogy-dna-database-criminal-investigations/599005/ [https://perma.cc/3S7E-E9T6].

121 *FamilyTreeDNA Law Enforcement Guide*, *supra* note 116.

122 *See* Zhang, *supra* note 120.

123 *See* Kristen V. Brown, *DNA Site That Thawed Cold Cases Sold as Forensics Business Booms*, BLOOMBERG (Dec. 11, 2019, 3:31 PM), https://www.bloomberg.com/news/articles/2019-12-11/dna-site-that-thawed-cold-cases-sold-as-forensics-business-booms [https://perma.cc/PWL3-3FA2].

124 *See* Maryland v. King, 569 U.S. 435, 462 (2013) ("The expectations of privacy of an individual taken into police custody 'necessarily [are] of a diminished scope.'" (alteration in original) (quoting Bell v. Wolfish, 441 U.S. 520, 557 (1979))).

125 *See* Schuppe, *supra* note 12 (discussing that parents were outraged that police had used their DNA to build a case against their son with genetic analysis).

126 *King*, 569 U.S. at 482 (Scalia, J., dissenting).

amassed genetic information in DTC company databases that dangerously approaches unchecked surveillance of highly personal information.[127]

II. Consent

Because law enforcement searches of DTC company databases are likely governed by the Fourth Amendment, consent can easily resolve this imbalance. Consent satisfies any Fourth Amendment concerns "because it is no doubt reasonable for the police to conduct a search once they have been permitted to do so."[128] The majority of legislation that even touches genetic privacy also revolves around informed consent principles.[129] Consent, if meaningful, thus offers a clear solution to privacy concerns. The remaining inquiry is whether consent is valid. This Part explains how consent works in a variety of contexts—including the Fourth Amendment's individual and third-party consent, digital consent, and medical procedure consent—and when that consent is or is not meaningful. In particular, this Part contrasts the lower levels of protection that the Fourth Amendment and digital consent affords privacy interests with the higher levels afforded by medical procedure consent.

A. Fourth Amendment

Fourth Amendment policy encourages individuals to consent to searches to aid the prosecution in solving crimes and protecting the public.[130] Where police lack probable cause, consent "may be the only means of obtaining important and reliable evidence,"[131] turning an otherwise invalid search into a constitutional one.[132] There are two types of consent under the Fourth Amendment: individual consent and third-party consent, the latter of which includes an inquiry into individual consent. This Section discusses each of these frameworks.

1. Third-Party Consent

Third-party consent allows law enforcement to access information about a suspect through the use of another person—the third party—regardless of whether the suspect has consented. Under third-party

127 Kolenc, *supra* note 111, at 102.

128 Florida v. Jimeno, 500 U.S. 248, 250–51 (1991) (citing Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973)).

129 *See supra* notes 95–99 and accompanying text.

130 *See* Coolidge v. New Hampshire, 403 U.S. 443, 488 (1971).

131 *Schneckloth*, 412 U.S. at 227.

132 *Id.* at 228.

consent, consent of another person, such as a consumer, who has "common authority over . . . effects is valid as against [an] absent, nonconsenting person" who shares that authority, such as a suspect.[133] This is because an individual who shares property with another assumes the risk that the co-owner will share the property with the police.[134] Common authority is determined by "mutual use of the property by persons generally having joint access or control for most purposes."[135] In assessing whether there is common authority, courts consider whether "widely shared social expectations" establish that the individuals may exercise their authority over the property in ways that affect each other's interests.[136]

Although property principles are not dispositive,[137] they can aid the inquiry into common authority.[138] With DNA, the most common belief is that each individual owns their personal DNA.[139] Consumer DNA databases also address property rights of DNA as an individual right.[140] DNA is communal, as it is shared with relatives.[141] Understanding this *sui generis* nature of DNA, Professor Natalie Ram proposes that DNA be analyzed as a tenancy by the entirety, in which each individual owns her entire DNA but shares ownership of the common portions of her DNA equally with her relatives.[142] Professor Erin Murphy has similarly agreed that the shared interest in DNA "could be likened to the joint interest held by property owners who share common space."[143] Although the general belief is that DNA is owned by an individual,[144] this is an attractive analysis and offers insight on how to think about DNA in the law. The shared nature of

133 United States v. Matlock, 415 U.S. 164, 170 (1974).

134 Georgia v. Randolph, 547 U.S. 103, 131 (2006) (Roberts, C.J., dissenting).

135 *Matlock*, 415 U.S. at 171 n.7.

136 *Randolph*, 547 U.S. at 111.

137 *See id.* at 110.

138 *See id.* at 110–11 (explaining that widely shared social expectations of whether an individual has common authority over some item "are naturally enough influenced by the law of property, but not controlled by its rules").

139 Jessica L. Roberts, *Progressive Genetic Ownership*, 93 NOTRE DAME L. REV. 1105, 1149–50 (2018).

140 *See id.* at 1129.

141 *Id.* at 1122.

142 *See* Natalie Ram, *DNA by the Entirety*, 115 COLUM. L. REV. 873, 906–10 (2015).

143 Erin Murphy, *Relative Doubt: Familial Searches of DNA Databases*, 109 MICH. L. REV. 291, 336 (2010). Not all scholars agree, however, that tenancy by the entirety is the best way to think about the shared nature of DNA. *See* Teneille R. Brown, *Why We Fear Genetic Informants: Using Genetic Genealogy to Catch Serial Killers*, 21 COLUM. SCI. & TECH. L. REV. 118, 166 (2020) (disputing the tenancy by the entirety idea because DNA is not real property and individuals need not obtain consent of family members when they undergo genetic testing).

144 Roberts, *supra* note 139, at 1149–50.

DNA is exactly what allows law enforcement to use it as an investigative tool. These searches could consequently directly implicate third-party consent doctrine.

2. *Individual Consent*

Even if a third party can consent to the search of an individual's property, that third party's consent must still be valid on its own. The typical standard for individual consent is whether the consent was given voluntarily given the totality of the circumstances.[145] The bar for achieving consent is low. This is because the U.S. Supreme Court held that consent does not require a literal knowing choice or knowledge of the right to refuse to consent.[146] Even in a case where law enforcement persuaded an individual to give his consent, a search was valid merely because, regardless of persuasion, the individual still voluntarily agreed to the search.[147] Another reason for this low bar is that the scope of the consensual search is limited to what a reasonable person would understand their consent to apply.[148] With this flexible standard, police can constitutionally conduct more expansive searches by carefully choosing how they request access.[149]

Contract principles can be helpful in determining whether an individual has consented to a suspicion-less search. For example, in *Dykes v. Southeastern Pennsylvania Transportation Authority*,[150] the Third Circuit Court of Appeals used contract principles to find that a drug and alcohol test required by a collective bargaining agreement was reasonable under the Fourth Amendment because the employee had consented to the process in the agreement.[151] In the technological age, courts are beginning to use contract principles to determine

145 Schneckloth v. Bustamonte, 412 U.S. 218, 227 (1973).

146 *See id*.

147 Davis v. United States, 328 U.S. 582, 593–94 (1946).

148 Florida v. Jimeno, 500 U.S. 248, 251 (1991).

149 4 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 8.1, at 4–5 (4th ed. 2004); Alexander A. Mikhalevsky, Note, *The Conversational Consent Search: How "Quick Look" and Other Similar Searches Have Eroded Our Constitutional Rights*, 30 GA. ST. U. L. REV. 1077, 1080 (2014) ("Police forces across the country have tested the limits of consent by asking vague, conversational questions to suspects with the goal of obtaining a suspect's consent to search, even though that individual may not want to allow the search or may not know that he or she has the right to deny consent."). For example, the Supreme Court found that a defendant's consent to police's request to search his car reasonably could extend to a search of the entire car, including packages within it. *See Jimeno*, 500 U.S. at 251.

150 68 F.3d 1564 (3d Cir. 1995).

151 *See id.* at 1568–70 (drawing the principle of reasonability of a search required by a collective bargaining agreement from *Bolden v. Southeastern Pennsylvania Transportation Authority*, 953 F.2d 807, 829 (3d. Cir. 1991)).

whether individuals have indeed consented to giving information over to others based on privacy policies in the digital context.[152]

B. Digital Consent

When it comes to general digital consent, there is less guidance. Ideally, consent is obtained from an "agreement[] between parties who have equal bargaining power, significant resources, and who *knowingly* and *voluntarily* agree to assume contractual or other legal obligations."[153] Digital consent models, however, generally fall short of the ideal model of consent[154] and do not appear to be meaningful. This is because these terms of service and privacy policies are contracts of adhesion.[155] A contract of adhesion arises when a contract "is not subject to negotiation and is offered by the more powerful party on a 'take it or leave it' basis."[156] Although courts generally enforce contracts of adhesion,[157] critics frequently argue that contracts of adhesion, such as corporate privacy policies, are not adequate to protect *privacy*.[158] This objection is likely because contracts of adhesion such as privacy policies involve what Professors Neil Richards and Woodrow Hartzog call "unwitting consent"[159]—consent that occurs when individuals do not understand "the legal agreement, . . . the technology being agreed to, or . . . the practical consequences or risks of agreement."[160]

These problems seem to particularly affect commercial DNA databases, where consent is provided through lengthy, and often complex, terms of service and privacy policies that consumers are unlikely to carefully read, making these consumers unlikely to know what submitting their DNA might cost them or others.[161] To remedy these

---

152 Wayne A. Logan & Jake Linford, *Contracting for Fourth Amendment Privacy Online*, 104 MINN. L. REV. 101, 104 (2019).

153 Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1463 (2019).

154 *Id.*

155 *See* Jay P. Kesan, Carol M. Hayes & Masooda N. Bashir, *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 424 (2013).

156 *Id.*

157 Alexandra L. Mitter, Note, *Deputizing Internet Service Providers: How the Government Avoids Fourth Amendment Protections*, 67 N.Y.U. ANN. SURV. AM. L. 235, 263–64 (2011).

158 *See* Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 YALE L.J. F. 8, 17 (2016).

159 Richards & Hartzog, *supra* note 153, at 1466 (emphasis omitted).

160 *Id.*

161 *See* Tashea, *supra* note 1; Arcabascio, *supra* note 39, at 129 ("Given the muddy and sometimes convoluted notice provided to consumers on DTC-GTC websites, individuals may

problems, any future agreement must therefore vividly and clearly describe any consequences associated with submitting their DNA such that a consumer has the knowledge and incentive to appropriately assess the request seriously.[162] This is exactly the rationale that allowed the U.S. District Court for the Southern District of New York to find that AOL Mail's express notice of the possible exposure to law enforcement could form the basis for a consensual search.[163] Despite the rationale that agreements should be clear, the standard for consent is still a low bar.

C. Medical Consent

The aforementioned consent standards contrast with the higher consent standards in the medical context, a particularly relevant context given the biological nature of DNA analysis. In the medical community, informed consent is the standard for any medical procedure.[164] Informed consent requires medical professionals to notify the patient of what medically will be done and the possible consequences before consent is valid.[165] A 1976 report produced by the U.S. Department of Health and Human Services ("HHS") National Commission for the Protection of Human Subjects of Biomedical and Be-

---

not consider the possibility that their genetic data may be used by law enforcement . . . ."); J. Lyn Entrikin, *Family Secrets and Relational Privacy: Protecting Not-So-Personal, Sensitive Information from Public Disclosure*, 74 U. MIAMI L. REV. 781, 861 (2020) ("[T]he [DTC company's] fine-print 'terms and conditions' govern the scope of the consumer's 'informed consent.'"); Alexis C. Madrigal, *Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days*, ATLANTIC (Mar. 1, 2012), https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/ [https://perma.cc/WA7F-4YVQ] (explaining that it would take, on average, seventy-six work days for a consumer to read all the privacy policies she encounters in a year). These terms of services and privacy policies also fail to explain the risks and benefits of genetic testing more broadly. *See* Brown, *supra* note 143, at 166. Indeed, a 2018 study found that DTC companies generally do not provide sufficient information for consumers to make an informed decision to provide their genetic information to a given company. *See* James W. Hazel & Christopher Slobogin, *Who Knows What, and When?: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies*, 28 CORNELL J.L & PUB. POL'Y 35, 66 (2018).

162 Richards & Hartzog, *supra* note 153, at 1492 ("To be meaningful, requests for consent must be infrequent, the risks of giving consent must be vivid and easy to envision[, such as imprisonment or exoneration], and data subjects must have an incentive to take each request seriously." (emphasis omitted)).

163 *See* United States v. DiTomasso, 56 F. Supp. 3d, 584, 597 (S.D.N.Y. 2014) (finding that because AOL explicitly warns users in its terms of service that it reserves the right to share private data with law enforcement in response to illegal behavior, it was reasonable to assume a person had consented to law enforcement's access to that data).

164 Natalie Ram, *Tiered Consent and the Tyranny of Choice*, 48 JURIMETRICS 253, 253 (2008).

165 *See* Planned Parenthood of Cent. Mo. v. Danforth, 428 U.S. 52, 67 n.8 (1976).

havioral Research[166] recommended that human subjects have the relevant information to make decisions, that they comprehend this information, and that they consent entirely voluntarily.[167] HHS codified these recommendations, requiring researchers to obtain consent only after informing human subjects of the procedures to be performed,[168] any risks or benefits,[169] and that participation is entirely voluntary and can be withdrawn at any time.[170] With these additional requirements, informed consent at least ensures that a literal knowing, and valid, choice can be made.

This is exactly why some scholars advocate for the import of informed consent from the medical context into the Fourth Amendment context more generally.[171] Professor Christo Lassiter argues that importing medical informed consent into the Fourth Amendment makes sense because, just like medical procedures, consent in Fourth Amendment searches of the person are grounded in the principles that individuals have control over their persons.[172] Just as uninformed consent fails to give authorization to invade a patient's body, uninformed consent to search someone's person therefore will fail to protect that individual's constitutional privacy.[173] The same idea can be applied to restore the balance between law enforcement searches of individual DNA voluntarily submitted to DTC companies.

III. Restoring Balance to DTC Company Database Searches

As established in Part I, law enforcement's access to DTC company databases gives law enforcement broad surveillance power at the expense of individual private interests.[174] This access results in an unconstitutional imbalance[175] that favors law enforcement needs over

166 The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of Research, Report of the National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research, 44 Fed. Reg. 23,192 (Apr. 18, 1979).

167 *See id.* at 23,194–95; Richards & Hartzog, *supra* note 153, at 1474.

168 Protection of Human Subjects: General Requirements for Informed Consent, 45 C.F.R. § 46.116(b)(1) (2019).

169 *Id.* § 46.116(b)(2)–(3).

170 *Id.* § 46.116(b)(8).

171 *See, e.g.*, Christo Lassiter, *Consent to Search by Ignorant People*, 39 Tex. Tech L. Rev. 1171, 1192–93 (2007) ("If informed consent is the standard in medicine for operation or treatment procedures affecting the medical person, the same standard makes sense for the constitutional person . . . .").

172 *See id.*

173 *See id.* at 1193.

174 *See supra* Sections I.B–.D.

175 At its most basic foundation, the Fourth Amendment seeks to balance the interests of

privacy interests with no legal constraints.[176] To establish balance between privacy and law enforcement interests, federal and state legislators should require DTC companies to include an explicit and informative option for individuals to opt out of law enforcement access while signing up for the service. With this consent, law enforcement may then legally access this specific pool of DNA and use it to investigate a suspect under third-party consent principles.[177] This Part explains this process and describes how the similarities between medical procedures and DNA analysis, the heightened need for protection in both contexts, and the individual and communal nature of DNA make the application of informed consent principles particularly appropriate for the DNA database search context.

A. Application

The opt-out framework operates in two connected parts: informed consent at the individual level and third-party consent as a tool to find a suspect. Federal and state legislatures can protect privacy interests by requiring informed consent before law enforcement can access a consumer's DNA. Given the highly personal and revealing nature of DNA and bodily integrity associated with that information, informed consent will ensure that adequate measures are taken to allow individuals to protect their own privacy.[178] This notice would appear on a separate webpage with an option to opt out of law enforcement access upon signing up for the DTC company database service.[179] This separate webpage would follow the type of informed consent that appears in the medical procedure context, requiring notice of the procedures to be performed,[180] any risks or benefits,[181] and that participation is entirely voluntary and can be withdrawn at any

law enforcement to protect society and apprehend criminals with the interests of citizens in protecting their privacy. *See* Maryland v. King, 569 U.S. 435, 448 (2013) (explaining that a court must weigh "'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy'" (alteration in original) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999))).

176 *See supra* Sections I.B–.D.

177 It is helpful to reestablish a common terminology for each component of this process. First, a "consumer" submits their DNA to a DTC company. Second, a "suspect" is implicated as a result of that consumer's actions and her DNA is ultimately found to match the crime scene.

178 *See supra* Section II.C.

179 *See* Ram, *supra* note 43, at 1362–63.

180 Protection of Human Subjects: General Requirements for Informed Consent, 45 C.F.R. § 46.116(b)(1) (2019).

181 *Id.* § 46.116(b)(2)–(3).

time.[182] The notice page would similarly explain that police can use this genetic information to investigate both that consumer and her family members, close or distant, for any connections to an unsolved crime and that this may result in further criminal action taken against the consumer or her family. The notice would then explain that even if that individual does stay in this pool, she can choose to opt out at any time in the privacy and security settings, upon which her genetic information will be immediately removed from the law enforcement pool. With these requirements, the consumer's consent would be more knowing and voluntary such that law enforcement searches of that data represent a valid consensual search.

In the interest of balancing the government and privacy interests under the Fourth Amendment, however, the nature of the agreements should still allow law enforcement to access *some* DNA data.[183] This objective is why the agreements would default to opting *in* to the portion of the database which law enforcement can access. Digital defaults are widely used by policymakers to encourage certain types of behavior, such as organ donations.[184] By making the standard default to opt in to law enforcement access, the government can encourage consumers to help law enforcement search for cold cases of violent crimes, a goal that the U.S. Supreme Court has acknowledged as important to ensure public safety.[185] And any concern that this default would fail to afford the user a valid choice[186] would be alleviated by

---

182 *Id.* § 46.116(b)(8).

183 *See* Solana Lund, Note, *Ethical Implications of Forensic Genealogy in Criminal Cases*, 13 J. BUS. ENTREPRENEURSHIP & L. 185, 196 (2020) ("[C]atching murders and solving cold cases is something that is widely supported for obvious reasons.").

184 Natalie Ram & Jessica L. Roberts, *Forensic Genealogy and the Power of Defaults*, 37 NATURE BIOTECHNOLOGY 707, 707 (2019).

185 *See* Coolidge v. New Hampshire, 403 U.S. 443, 488 (1971) (explaining the value of encouraging consent to law enforcement search to help ensure public safety). Some have called for a ban on law enforcement's use of DTC company databases altogether, arguing that there is no way to protect privacy interests and allow law enforcement access. *See* Arcabascio, *supra* note 39, at 147; Najla Hasic, Note, *An Invasion of Privacy: Genetic Testing in an Age of Unlimited Access*, 44 S. ILL. U. L.J. 519, 550 (2020). Such a ban, however, would invert the balance in favor of privacy interests, which is not the objective of the Fourth Amendment, *see supra* note 175 and accompanying text, and is unnecessary given the limitations to access laid out in this Note, *see supra* Section III.C.2.

186 *See* Hasic, *supra* note 185, at 550; Lund, *supra* note 183, at 202–03. Requiring an opt-in choice, rather than an opt-out choice as this Note offers, would also unduly invert the balance toward privacy interests. When GEDmatch changed its policy to require users to affirmatively opt in to a law enforcement pool, the amount of data law enforcement could use plummeted from 1.4 million to 140,000. *See* Katelyn Smith, *Genealogy Database Privacy Change Creates Challenges for Investigators*, WGAL NEWS 8 (Sept. 6, 2019, 6:58 PM), https://www.wgal.com/article/genealogy-database-privacy-change-creates-challenges-for-investigators/28945357#

the informed consent a consumer must provide to allow law enforcement to retain access.

This consent then would apply under third-party consent principles against another member of a consumer's family—the suspect—because the consumer and the suspect can be considered to legally share common authority over their shared DNA.[187] This common authority derives both from widely shared societal expectations and property concepts. As an initial matter, widely shared societal expectations indicate that individuals can consent to searching even the shared portions of their DNA. Most individuals believe that they have the right to do what they please with their own DNA, much like how they believe they have the right to do what they please with their own body.[188] It would be reasonable for law enforcement to believe that if a consumer consents to the search of her DNA, she consents to the search of *all* of her DNA, including that which she shares with her relatives.[189] Society would therefore recognize that a consumer has common authority in the shared portion of her DNA.

As for property concepts, although property concepts are not dispositive to the common authority inquiry, they are persuasive.[190] Professor Ram's tenancy by the entirety concept describes DNA in terms of joint occupancy where each relative who possesses familial DNA has the individual right to do whatever she wants with her DNA, even the shared portions, including pursuing genetic testing without familial consent.[191] Applying Professor Ram's tenancy by the entirety concept of DNA to the Fourth Amendment, any relative, therefore, has common ownership over the portion of DNA she shares with the rest of her family and thus can consent to law enforcement searching that shared portion of DNA. By looking to both property principles and widely shared societal expectations, common authority and thus valid third-party consent is established.

[https://perma.cc/3MLR-PVXW]. Although this Note does not advocate for the former unfettered access, a more measured balance is the objective. *See supra* note 175 and accompanying text.

187 Consent of one person is valid against another person if that person has common authority over the item searched. United States v. Matlock, 415 U.S. 164, 170 (1974).

188 *See* Roberts, *supra* note 139, at 1150.

189 This is similar to the idea that if an individual consents to the search of her car, she consents to the search of every part of her car that evidence could be found. *See* Florida v. Jimeno, 500 U.S. 248, 251 (1991) ("The scope of a search is generally defined by its expressed object."); LaFave, *supra* note 149, at 4–5.

190 *See supra* notes 137–38 and accompanying text.

191 Ram, *supra* note 142, at 935.

B. Justifications

Individual and third-party consent are the most appropriate doctrines to apply because they adequately encompass the biological, communal, and individual nature of DNA. Importing informed consent requirements from the medical context is appropriate because of the similarities between bodily integrity in medical procedures and privacy in one's biological information under the Fourth Amendment.[192] Just as consent in the medical context seeks to ensure that medical procedures do not affront someone's interest in her own body,[193] similarly, consent in the Fourth Amendment context is grounded in the idea that people have the right against government intrusions into their bodily privacy.[194] Because DNA is a highly revealing part of the body, it is undoubtedly appropriate to implement a heightened standard of consent to ensure the same bodily integrity and privacy. Indeed, a number of commentators support adding informed consent requirements to DTC companies.[195]

Applying third-party consent doctrine to DTC company database searches is also appropriate because it encompasses the unique nature of DNA as well as provides a simple analytical framework that allows police and trial judges to evaluate the validity of the search. DNA is unique in that it is distinct to each person yet shared by relatives:

> Genetic data is simultaneously personal and communal. It can communicate sensitive information about an individual, including a person's ancestry, familial relationships, presence at a crime scene, medical risk, and perhaps even behavioral tendencies. Yet at the very same time, human beings are 99.9% genetically similar, with even greater levels of homogeneity among family members.[196]

In light of this simultaneous individual and communal nature, traditional notions of privacy rights under the Fourth Amendment will lead to issues of standing[197] and general neglect of how one person's

---

192 *See* Lassiter, *supra* note 171, at 1192–93.

193 *Id.*

194 *Id.*

195 *See, e.g.*, McFerrin, *supra* note 104, at 996–97; Brown, *supra* note 143, at 177–82; Entrikin, *supra* note 161, at 867; Lund, *supra* note 183, at 203; Jamie M. Zeevi, Note, *DNA Is Different: An Exploration of the Current Inadequacies of Genetic Privacy Protection in Recreational DNA Databases*, 93 ST. JOHN'S L. REV. 767, 806–08 (2019).

196 Roberts, *supra* note 139, at 1122 (footnotes omitted).

197 *See* Dery, *supra* note 8, at 139–43.

DNA implicates another person's,[198] making traditional analyses unsuited to DTC company database searches. Understanding genetic data in terms of communal-centric doctrine, such as third-party consent doctrine, will more accurately reflect the individual and shared nature of the information.[199]

Policy reasons also justify applying third-party consent doctrine to DTC company database searches. Consensual searches have an administrability advantage that allows the police and courts to more easily determine the validity of the search.[200] A judge need only determine whether the third party validly gave consent to find whether the search was valid.[201] With the help of informed consent legislation, this inquiry will be fairly straightforward and standardized.[202] Consent doctrine, therefore, provides a straightforward inquiry for evaluating a largely complicated and messy web of privacy interests at stake in DTC company database searches.

C. Responses to Criticisms

Critics might be concerned about the validity of what might appear to be a contract of adhesion, the scope of such consensual DNA searches, and the appropriateness of applying shared consent to shared DNA given that DNA is so personal. All three concerns, however, can be remedied. This Section addresses each in turn.

1. Contracts of Adhesion

Critics might be concerned that this informed consent agreement is a contract of adhesion and therefore an inadequate protection of privacy rights. A contract of adhesion involves a less powerful party, usually a consumer, accepting terms as the more powerful party, usually a company, writes them.[203] Contracts of adhesion inadequately protect privacy rights not because they do not allow individuals to voluntarily consent,[204] but rather because contracts of adhesion are

198 *See* Ram, *supra* note 142, at 876–77 (explaining that legal actors have failed to account for how one's DNA affects her relative's).

199 *See* Roberts, *supra* note 139, at 1161.

200 This is because if there is valid consent, the search is presumptively reasonable. Florida v. Jimeno, 500 U.S. 248, 250–51 (1991) (citing Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973)).

201 *See id.*

202 *See supra* Section III.A.

203 Kesan et al., *supra* note 155, at 424.

204 *See supra* Section II.B.

marked by their "take it or leave it" nature[205] with no room for individuals to retain the service while still rejecting consent to search. An informed consent agreement, on the contrary, offers consumers the option to reject consent to law enforcement access to their DNA without having to forego the genetic testing service altogether.[206] By ensuring that DTC companies obtain this consent separately from the terms of service, legislators can also ensure that this consent does not arise merely from a vague sentence in a multi-page terms of service.[207] With these features, checking a box will not preclude valid consent.

2. Scope

Critics are also concerned with the sheer multitude of relatives that one individual's consent might reach.[208] With this broad reach inherent in DTC company databases, it is easy to argue that one person's consent to law enforcement search will impermissibly allow law enforcement to search the millions of distant and not-so-distant relatives connected to that person from the past, present, and future.[209] Although this concern is justified, the scope of what information law enforcement can access is not unlimited and their access can be narrowed according to current principles of the scope of consensual searches.

In *Florida v. Jimeno*,[210] the U.S. Supreme Court established that consent extends only so far as to where a reasonable person would understand the consent to extend.[211] It was therefore reasonable for the police to also search a container inside Jimeno's car because Jimeno consented to the search of his car without clarifying that the search should not extend to everything inside it.[212] When a defendant consents to the search of his garage, however, the Court has stated that the consent does not extend to the search of his house because the house is separate from the garage.[213] Similarly, DTC company database searches can be limited to where reasonable people would assume the consumer's consent extends.

---

205 Kesan et al., *supra* note 155, at 424.

206 *See supra* Section III.A.

207 *See* Richards & Hartzog, *supra* note 153, at 1471.

208 *See, e.g.*, Dery, *supra* note 8, at 132–33.

209 *See* Guest, *supra* note 29, at 1050.

210 500 U.S. 248 (1991).

211 *Id.* at 251.

212 *See id.*

213 Walter v. United States, 447 U.S. 649, 656–57 (1980).

To locate this limit, one can again look to commonly held beliefs about the nature of DNA. People generally believe that an individual owns her own DNA.[214] It is therefore reasonable to assume that when individuals consent to a law enforcement search of their DNA for matches, they only give consent to search for matches to the crime scene DNA, not their entire family lines' DNA. Accordingly, although it certainly would be feasible to inspect shared DNA as far out as fifth cousins,[215] under the *Jimeno* Court's reasoning, police would only be legally allowed to search DNA for how it overlaps with the crime scene DNA, not any additional DNA that might belong to nonsuspect relatives who have foregone entry into the law enforcement pool.[216]

3. The Propriety of Common Authority in Shared DNA

Critics of the third-party doctrine as applied to DTC databases also argue that people cannot have common authority over shared DNA because relatives do not assume the risk that other relatives can expose that shared DNA to the police.[217] Transmitting DNA through birth is an entirely involuntary process and it might be unreasonable to say that an individual assumes the risk that another relative will expose her shared DNA to law enforcement merely by having a biological relation.[218] Given that third-party consent is grounded in the

---

214 *See* Roberts, *supra* note 139, at 1150 (describing a commonly held intuition that individuals own their own genetic information).

215 Fifth cousins share 0.05% of DNA, compared to the 50% that parents share with their children or siblings share with each other. *Average Percent DNA Shared Between Relatives*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/212170668-Average-percent-DNA-shared-between-relatives [https://perma.cc/9MQF-YSJF].

216 Relatedly, an additional issue with law enforcement accessing DTC company databases, in "which [the genetic information] can be retained indefinitely, is the duration of consent." Joseph (Joe) Zabel, *The Killer Inside Us: Law, Ethics, and the Forensic Use of Family Genetics*, 24 BERKELEY J. CRIM. L. 47, 83–85 (2019). With the only guidance from the U.S. Supreme Court being that the consent must be reasonable, *see Jimeno*, 500 U.S. at 251, the contours of this limitation on consent is unsettled among lower courts. *Compare, e.g.*, Tucker v. Williams, 682 F.3d 654, 659–60 (7th Cir. 2012) (finding that plaintiff's consent, derived from the sentence "go ahead and take it then," to defendant's seizure of a backhoe that occurred two months later was valid because a reasonable person would understand the consent to be indefinite), *with* United States v. Escamilla, 852 F.3d 474, 484–85 (5th Cir. 2017) (finding that even though defendant consented to an agent looking through his phone and never revoked his consent nor affirmatively limited the scope of the search to that instant, a second search of the phone four hours later was invalid because the circumstances suggested that a reasonable person would understand the consent to be limited to the first instance). An analysis of how consent should be limited in time, both generally and specifically regarding DTC company database searches, could be the topic of a separate Note, and therefore is not addressed here.

217 *See, e.g.*, Dery, *supra* note 8, at 132; Murphy, *supra* note 143, at 336; Zabel, *supra* note 216, at 90–91.

218 *See, e.g.*, Dery, *supra* note 8, at 132; Murphy, *supra* note 143, at 336–37.

idea that because an individual who shares property assumes the risk that her co-owner will share that property or information with the police then that co-owner's consent is valid against her, third-party consent is therefore inapplicable.[219]

Although this is a rational objection, the assumption of risk theory that underlies the Court's third-party consent jurisprudence does not always carry the day. What establishes the requisite common authority in third-party consent doctrine is the "*mutual use* of the property by persons generally having *joint access or control* for most purposes."[220] Mutual use of the object searched and joint access or control over the object searched are therefore key in determining common authority.[221] Using this inquiry, lower courts have found that parents and children can consent to searching the house they share because of the mutual use of and joint access to the house.[222] Children and their parents likely do not have much of a say over their joint occupancy given general societal and biological expectations that parents should care for their children in a house together. In some ways, one can say that this too establishes common authority by virtue of a biological relation. Likewise, the absence of an assumption of risk in DNA sharing is not dispositive nor evidence of a lack of common authority.

Exposing a family members' privacy while giving up one's own privacy is also not entirely uncommon.[223] Orin Kerr describes several helpful examples:

> A family member with the same last name might post their home address on the web or in the phone book. If someone wants to find you, a quick google search of your last name may give people an inkling of where you live because of what your family member posted. Or say you don't want a picture of you to be online. You don't post one, but a friend or colleague might post a public picture of a group of people that

---

219 *See, e.g.*, Dery, *supra* note 8, at 132–33; *see also* Georgia v. Randolph, 547 U.S. 103, 113 (2006) (explaining that consent by one co-occupant cannot overcome affirmative nonconsent of another co-occupant).

220 United States v. Matlock, 415 U.S. 164, 171 n.7 (1974) (emphasis added).

221 *See id.*

222 *See, e.g.*, United States v. Rith, 164 F.3d 1323 (10th Cir. 1999) (finding a parent could consent to search of eighteen-year-old child's room); United States v. Clutter, 914 F.2d 775, 778 (6th Cir. 1990) (finding twelve- and fourteen-year-old children could validly consent to inspection of house that belonged to parents).

223 *See* Orin S. Kerr, *Tentative Thoughts on the Use of Genealogy Sites to Solve Crimes*, VOLOKH CONSPIRACY (May 2, 2018, 4:27 AM), https://reason.com/volokh/2018/05/02/tentative-thoughts-on-the-use-of-geneolo/ [https://perma.cc/HJH5-33ST].

> includes you without your permission. As a practical matter, maintaining privacy often requires the cooperation of others.[224]

Yet, no one could likely question your authority to put your own address or photo online, as you yourself are the partial inhabitant of the address or the partial subject of the photo.[225] Professor Teneille Brown offers another example: In an autobiography, an author shares her own story while also necessarily telling the stories of those she is close to, often without their consent.[226] The analog to DNA databases is readily apparent. Much like with the photo, the home address, or the autobiography, because of the shared quality of DNA, each individual has the authority to expose their own DNA to police while inadvertently exposing some private information of a family member.[227]

The application of third-party consent to DTC company database searches is therefore an easily administrable and suitable doctrine that will ensure both the validity of the search and the ability of law enforcement to solve cold cases.

Conclusion

DTC companies are only increasing in popularity, which means law enforcement will soon have unfettered access to the entire public's genetic information. This possibility dangerously resembles a surveillance state that values crime solving at the cost of individual privacy. The Fourth Amendment was designed specifically to prevent any undue cost of individual privacy, and it is the Fourth Amendment in conjunction with other legal principles that legislators must consider if they want to prevent this panopticon. Legislators are in the best place to combine these legal principles because they can go beyond the Constitution to provide additional safeguards of liberty. By using the heightened standard of informed consent in the scope of Fourth Amendment consent, legislators can ensure that every piece of DNA used by the police is done so with consent. As a result, legislators can guarantee law enforcement can do their job without stripping individuals of their privacy.

---

224 *Id.*

225 *Id.*

226 *See* Brown, *supra* note 143, at 168–70.

227 *See id.* at 165 ("When I choose to obtain genetic tests to complete my genetic story, . . . I am writing *my* story. I am gathering information and sharing it because it is my autonomous choice[, even though] [t]his decision might indirectly implicate the privacy of others, and it might hurt them.").