Winter 2020

A Genetic Surveillance State: Are We One Buccal Swab Away from A Total Loss of Genetic Privacy?

Catherine Arcabascio
Nova Southeastern University - Shepard Broad Law Center, arcab.c@nova.edu

A Genetic Surveillance State: Are We One Buccal Swab Away From a Total Loss of Genetic Privacy?[1]

CATHERINE ARCABASCIO

INTRODUCTION:

To date, over 15 million people have submitted their genetic sample to a Direct-To-Consumer Genetic testing company ("DTC-GTC").[2] A person's genetic data is the most fundamental private information one can possess. That makes it an incredibly powerful tool because an enormous amount of information can be gleaned from a tiny sample of saliva or other bodily secretion. "Genomic data is special, since it encodes not only our blueprint, *but that of our family and children.* The continuing privacy and the security of people's genetic data, both immediately, and into the long term, is of paramount importance." (Emphasis added)[3] "A genome is not your average piece of data—it is inherently identifiable, it is familial (revealing your genomic data can reveal sensitive information about your family mem-

1. Catherine Arcabascio is a Professor of Law at Nova Southeastern University, Shepard Broad College of Law. She is a former Brooklyn Assistant District Attorney and also served as the Director of the Florida Innocence Project, which she co-founded. A heartfelt thanks to Research Assistants Tonja Vucetic, Yesnela Rodriguez, Elaine Martin, and Bradley Denniston for their assistance.

2. "More than 15 million people have submitted their DNA to companies like FamilyTreeDNA, 23AndMe and Ancestry.com in recent years. While they represent a small fraction of all people, the pool of profiles is large enough to allow 60 percent of white Americans — the primary users of DNA sites in the United States — to be identified through the databases, according to researchers." Heather Murphy, *Most White Americans' DNA Can Be Identified Through Genealogy Databases*, N.Y. TIMES (Oct. 11, 2018), https://www.nytimes.com/2018/10/11/science/science-genetic-genealogy-study.html?module=inline. These companies have been referred to in articles and other literature as either DTC-GT's or DTC-GTCs. For consistency, this article will use DTC-GTC. However, direct quotes from other sources that contain DTC-GT will not be changed.

3. Lauren Friend, *Direct-to-Consumer Genetic Testing*, KPMG GLOBAL STRATEGY GROUP 1, 2 (2018), https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/08/direct-to-consumer-genetic-testing.pdf.

bers as well), and its value is long-lasting."[4] The privacy concern has even moved the Department of Defense to issue a warning to its employees regarding the use of DTC-GTCs. In December 2019, the Office of the Secretary of Defense issued a memorandum advising its employees not to use such companies. Among other concerns, it stated, ". . .there is increased concern in the scientific community that outside parties are exploiting the use of genetic data for questionable purposes, including mass surveillance and the ability to track individuals without their authority or awareness."[5]

During the past several years, there has been a steep rise in DTC-GTCs that are utilized by individuals who are curious about their ancestry, possible genetic disease markers, or tracking down unknown living relatives. Some of these individuals have also taken their genetic testing results from the DTC-GTCs and submitted the results to open source genealogical websites like GEDmatch that focus exclusively on genealogical research.[6] In some consumers, the curiosity about their ancestry seems to be irresistible. Others seek answers to legitimate questions about paternity or genetic markers for disease. In either case, those questions have driven the urge to submit one's most private, unique genetic sample to a mostly unregulated and ever-growing "private" database industry, one that now contains millions of DNA samples.[7]

By now, the names of these companies are familiar. Ancestry.com and 23andMe are the two most recognizable given the heavy marketing campaigns they continue to conduct to date.[8] It appears

4. Dana A. Elfin, *DNA Testing? You Might Want to Wait for More Legal Protection*, BLOOMBERG LAW (Jan. 7, 2019, 5:40 AM), https://news.bloomberglaw.com/pharma-and-life-sciences/DNA-testing-you-might-want-to-wait-for-more-legal-protection.

5. Shawn Snow, *Pentagon advises troops to not use consumer DNA kits, citing security risks*, MILITARY TIMES (Dec. 24, 2019), https://www.militarytimes.com/2019/12/24/pentagon-advises-troops-to-not-use-consumer-dna-kits-citing-security-risks/.

6. *See* Sarah C. Nelson, *Consumer Genetic Testing Customers Stretch Their DNA Data Further With Third-Party Interpretation Websites*, THE CONVERSATION (June 13, 2019, 11:06 AM), http://theconversation.com/consumer-genetic-testing-customers-stretch-their-DNA-data-further-with-third-party-interpretation-websites-118248.

7. *See generally 23andMe DNA Test Customer Reviews*, AMAZON, https://www.amazon.com/23andMe-DNA-Test-Ancestral-Opt/dp/B01LZ5K87Z/ref=sr_1_3?crid=14B9Q3ZFJPV6A&keywords=23andme+DNA+testing+kit&qid=1564425377&s=gateway&sprefix=23and%2Caps%2C154&sr=8-3#customerReviews (last visited July 29, 2019); AncestryDNA: *Genetic Ethnicity Test Customer Reviews*, AMAZON, https://www.amazon.com/AncestryDNA-Genetic-Ethnicity-Test/dp/B00TRLVKW0/ref=sr_1_1_sspa?crid=14B9Q3ZFJPV6A&keywords=23andme+DNA+testing+kit&qid=1564426067&s=gateway&sprefix=23and%2Caps%2C154&sr=8-1-spons&psc=1#customerReviews (last visited July 29, 2019).

8. *See 23andMe Launches First National TV Campaign*, 23ANDME (Aug. 5, 2013), https://mediacenter.23andme.com/press-releases/poh_ad_campaign/ (23andMe started its television ad-

that DTC-GTCs are spending quite a bit of money marketing their services to those who want to know where their families originated from, who their relatives are, or what kind of genes they carry for certain diseases for a minimal amount of money. As of 2017, 23andMe has been able to market different types of tests that identify genetic markers for illnesses such as Parkinson's, and Alzheimer's to name a few.[9] The marketing push and the low cost of testing is not surprising because the real value of their business is in the extraordinary amount of genetic data they possess and can sell, thereby translating into enormous current and future profits.[10] Moreover, there are currently hundreds of private DNA testing companies, as well as some other free public genetic-matching companies, that provide services other than actual testing to consumers.[11] Additionally, in order to access these sites, consumers must consent to a host of activities by these DTC-GTCs through a lengthy and often muddy set of notices.[12]

Thus, it is of no surprise that the proliferation of DNA samples accumulated by these private, largely unregulated, companies and organizations have caught the eyes of law enforcement. With millions of private citizens using them, law enforcement has seized the ability to obtain genetic information of innocent citizens so that they can create familial trees from that information to create a list of suspects in either existing or cold cases. Once a law enforcement organization is

---

vertising campaign in 2013); *see also* Tara Goodin, *FDA Allows Marketing of First Direct-to-Consumer Tests That Provide Genetic Risk Information For Certain Conditions*, U.S. FOOD & DRUG ADMINISTRATION (Apr. 6, 2017), https://www.fda.gov/news-events/press-announcements/fda-allows-marketing-first-direct-consumer-tests-provide-genetic-risk-information-certain-conditions (in 2017, the FDA allowed 23andMe it to market some of its genetic tests for certain diseases).

9. Tara Goodin, *FDA Allows Marketing of First Direct-to-Consumer Tests That Provide Genetic Risk Information For Certain Conditions*, U.S. FOOD & DRUG ADMINISTRATION (Apr. 6, 2017), https://www.fda.gov/news-events/press-announcements/fda-allows-marketing-first-direct-consumer-tests-provide-genetic-risk-information-certain-conditions.

10. *See* Lindsey Jones, *FDA Regulation Defines Business Strategy in Direct-to-Consumer Genetic Testing*, BIOTECH CONNECTION (Oct. 30, 2017), https://biotechconnectionbay.org/viewpoints/fda-regulation-defines-business-strategy-in-direct-to-consumer-genetic-testing/ (the diversifying reasons for consumer interest in DTC genetic testing are estimated to increase its global market value to $350 million by 2022).

11. 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, 35 (2018).

12. *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, 39 (2018) ("[w]ith some notable exceptions, these companies provided little or none of the information required for consumers to make informed decisions about their privacy . . . [including the] privacy implications of genetic testing, disclosing health information, and third parties gaining access to an individual's genetic information").

able to submit their samples to these databases, they can build a DNA family tree that includes family members who are related as far as the 9th degree.[13] Law enforcement's access to these private databases raise serious privacy concerns not only for those that submit the samples to the DTC-GTCs, but every member of that family, either living or not yet born.

Current privacy laws such as the Health Insurance Portability and Accountability Act ("HIPAA") and the Genetic Information Nondiscrimination Act ("GINA") simply do not offer sufficient protection in the DTC-GTC and genealogy research industries, especially against law-enforcement's uses. The Federal Trade Commission ("FTC"), which is responsible for consumer protection could play a greater role, but not if it merely applies the same regulations to DNA samples and data that it does to online sales of typical consumer products such as clothing and electronics. More importantly, current Fourth Amendment jurisprudence does not offer sufficient protection either. What consumers are left with is a largely unregulated industry that does not, and cannot, robustly guarantee the privacy rights of its users and any other potential stakeholders.

This article will explore these issues and provide suggestions on how to curb the increasing lack of privacy in genetic data, with a focus on law enforcement use. Part II of this article starts by providing background information about the more well-known DTC-GTCs and genetic research companies. Part III of this article sets forth the general genetic privacy issues that arise when consumers use DTC-GTCs and genetic research sites, discusses genetic regulation and genetic management issues, including DTC-GTCs attempts at self-regulation, consent, anonymity and deidentification concerns. Part IV discusses genetic privacy and the Fourth Amendment. Part V concludes with commentary and suggested solutions to the privacy issues raised.

I. DTC-GTCs

The most well-known and largest DTC-GTCs are Ancestry.com and 23andMe.com, but there are over 250 of such companies.[14] Ac-

13. SNAPSHOT DNA ANALYSIS, https://snapshot.parabon-nanolabs.com/#kinship (last visited Aug. 31, 2019).

14. Lauren Friend, *Direct-to-Consumer Genetic Testing*, KPMG GLOBAL STRATEGY GROUP (Aug. 2018), https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/08/direct-to-consumer-genetic-testing.pdf; Hazel & 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, 43–44 (2018).

cording to a KPMG report, the global DTC-GTC market value is expected to be valued more than one billion dollars by 2020.[15] Ancestry.com started as Ancestry Publishing and has its roots in a genealogy magazine, but it was not until 2002 that Ancestry.com began providing DNA testing to consumers.[16] By 2018, it had over 10 million DNA profiles in its database and, according to its website, became the largest in the world.[17]

23andMe was founded in 2006 and according to its website, has "over 5 million genotyped customers."[18] Ancestry.com's focus is on the use of DNA for genealogical purposes. On the other hand, 23andMe not only does genealogical testing, but offers a wide variety of genetic testing for disease markers.[19] 23andMe is the only DTC-GTC that has been approved by the FDA to do more advanced genetic testing for certain disease markers.[20]

Increasingly, "Americans now turn to DTC-GT companies in an attempt to translate their genetic data into insights into their health, ancestry and family relationships, lifestyle, as well as an ever-growing number of additional areas."[21] The process is simple. A testing kit can usually be purchased online at either their site or at sites like Amazon.com.[22] Testing prices vary, but the average test kit price for 23andMe, ranges from $99.99-199.00 (depending on where the consumer purchases it and whether there are sales).[23] For example,

---

15. Lauren Friend, *Direct-to-Consumer Genetic Testing*, KPMG GLOBAL STRATEGY GROUP (Aug. 2018), https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/08/direct-to-consumer-genetic-testing.pdf; *see generally* KPMG (2019), https://home.kpmg/xx/en/home.html (last visited July 29, 2019) (Klynfeld, Peat, Markwick, Goerdeler or KPMG, is a global accounting firm and part of the "big five" of accounting firms).

16. *We Help Unlock New Understanding and Meaningful Connections*, ANCESTRY (2019), https://www.ancestry.com/corporate/about-ancestry/our-story (last visited July 29, 2019).

17. *Id.*

18. *23andMe Statistics, Facts & History*, REVIEW CHATTER (Nov. 13, 2018), https://www.reviewchatter.com/statistics-facts-history/23andme.

19. *See* Rebecca Armstrong, *Best DNA Testing Kit 2019: Unravel Your Ancestry*,TOP TEN REVIEWS (July 16, 2019), https://www.toptenreviews.com/best-DNA-testing-kits.

20. *See Lists of Direct-To-Consumer Tests with Marketing Authorization*, U.S. FOOD & DRUG ADMINISTRATION (Nov. 1, 2018), https://www.fda.gov/medical-devices/vitro-diagnostics/direct-consumer-tests#list.

21. 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, 37 (2018).

22. Zina Kumok, *What to Know Before You Buy a DNA Test*, MAGNIFY MONEY (Apr. 13, 2018), https://www.magnifymoney.com/blog/news/DNA-tests-23andme-ancestryDNA-helix 1444682914/.

23. *See Find Out What Your DNA Says About Your Health, Traits and Ancestry*, 23ANDME, https://www.23andme.com/DNA-health-ancestry/?utm_source=google&utm_medium=search_shopping&utm_campaign=US_evergreen_sales_prs_shopping_h+a&gclid=EAIaIQobChMI66n

23andMe ran a Father's Day special that provided ancestry testing for just $50.[24] On average, however, it costs about $99 to run a DNA sample and get simple ancestry information.[25] Other more in depth testing for genetic markers for certain diseases can run about $199.[26]

After purchasing the testing kit, it is mailed to the consumer, who then usually provides either a buccal swab or a saliva sample and returns the kit for testing.[27] The DTC-GTC will then post the results of the test online.[28]

Ancestry.com and 23andMe.com run a heavy advertising rotation.[29] In 2016, it was reported that Ancestry.com spent $109 million and 23andMe spent $21 million in advertising.[30] 23andMe in particular has targeted younger audiences. In 2017, it ran an ad campaign in conjunction with the movie, *Despicable Me 3*, where the character Gru, does a 23andMe genetic test and ultimately finds out that he has a brother.[31]

In 2018, 23andMe also ran an aggressive marketing campaign and was the primary sponsor for the Billboard Music Awards.[32] During

---

Ym8254wIVCdbACh0BMAkiEAQYAiABEgKoQ_D_BwE&gclsrc=aw.ds (last visited July 29, 2019) (sale price of $199.00); 23andMe Personal Ancestry DNA Test Kit-Lab Fee Included, TARGET, https://www.target.com/p/23andme-personal-ancestry-DNA-test-kit-lab-fee-included/-/A-53450926 (last visited July 29, 2019) (sale price of $99.99).

24. Haley Henschel, *23andMe Father's Day Sale: Save $50 on Amazon*, MASHABLE (June 12, 2019), https://mashable.com/shopping/deal-june-12-23andme-health-and-ancestry-kits-on-sale-amazon/.

25. Tina H. Saey, *What I Actually Learned About My Family After Trying 5 DNA Ancestry Tests*, SCIENCE NEWS (June 23, 2018), https://www.sciencenews.org/article/family-DNA-ancestry-tests-review-comparison.

26. Lydia Ramsey, *I Revisited My 23andMe Results That Can Now Tell Whether You May Have an Increased Risk of Cancer – Here's What it Was Like*, BUSINESS INSIDER (Nov. 23, 2018, 8:39 AM), https://www.businessinsider.com/review-of-23andmes-new-genetic-health-risks-reports-2017-4.

27. *Should You Get a Home Genetic Test?*, HARVARD HEALTH PUBLISHING (Feb. 2019), https://www.health.harvard.edu/staying-healthy/should-you-get-a-home-genetic-test.

28. 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, 38 (2018).

29. *See Ancestry TV Commercials*, ISPOT.TV (2019), https://www.ispot.tv/brands/dhv/ancestry (last visited July 29, 2019) (for how many Ancestry TV ad campaigns aired in the past 30 days); *see also 23andMe TV Commercials*, ISPOT.TV (2019), https://www.ispot.tv/brands/Ias/23andme (last visited July 29, 2019) (for how many 23andMe TV ad campaigns aired in the past 30 days).

30. Antonio Regalado, *2017 Was the Year Consumer DNA Testing Blew Up*, MIT TECH. REV. (Feb. 12, 2018), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-DNA-testing-blew-up/.

31. *See* Ace Metrix, *23andMe- "Gru's 23andMe Genetic Journey"*, YOUTUBE (Dec. 8, 2017), https://www.youtube.com/watch?v=OIaF-b5yQxs.

32. Ne-Yo, FACEBOOK (May 20, 2018), https://www.facebook.com/NEYO/videos/teamed-up-with-23andme-the-billboard-music-awards-this-year-awesome-to-share-wit/10156050679657012/.

the holidays, these marketing campaigns offer even more discounted rates so more people will give the tests as gifts. As of January 2019, more than 26 million people had added their genetic profile to one of four (Ancestry.com, 23andMe, FamilyTreeDNA, MyHeritage) DTC-GTCs.[33] The rapid growth of the use of these DTC-GTCs is driven by the consumer's curiosity and self-empowerment.[34] "A sense of empowerment is a key driver of DTC-GT uptake – 80% of early adopters of DTC-GTC services report a sense of empowerment from their results, and claim 'curiosity' as a primary motivation. In response, 90% of DTC-GT companies use the emotional appeal of 'empowerment' in their marketing strategies."[35]

Other companies, such as GEDmatch are free, but do not offer genetic testing.[36] Rather, once consumers get their DNA tested by companies such as Ancestry.com and 23andMe, they can upload their raw DNA data to GEDmatch and do genealogical comparisons.[37] GEDmatch users can then potentially connect with other users who may be related. The reverse is not true. A consumer cannot upload data from another source to Ancestry.com or 23andme.

Thus, it should come as no surprise that these large DTC-GTCs have assembled massive databases. Ancestry.com and 23andMe alone contain the genetic data of over five million and two million customers, respectively.[38] What that effectively means is that in the near future, if left unregulated, almost every person living in the U.S of European descent ultimately will be identified through the irrelatives using a DTC-GTC or a genealogical website like GEDmatch.[39] In

33. Antonio Regalado, *More Than 26 Million People Have Taken an at-Home Ancestry Test*, MIT TECH. REV. (Feb. 11, 2019), https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/.

34. Loredana Covolo et al., *Internet-Based Direct-to-Consumer Genetic Testing: A Systematic Review*, 17(12) J. MED. INTERNET RES. (Dec. 14, 2015), https://www.jmir.org/2015/12/e279/.

35. Lauren Friend, *Direct-to-Consumer Genetic Testing*, KPMG GLOBAL STRATEGY GROUP (Aug. 2018), https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/08/direct-to-consumer-genetic-testing.pdf.

36. *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.

37. *GEDmatch*, YOUR DNA GUIDE, https://www.yourDNAguide.com/upload-to-gedmatch (last visited July 29, 2019).

38. 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, 44 (2018).

39. *Within a Few Years, 90% of Americans of European Descent Will Be Identifiable from DNA Through Genealogy Sites*, KAISER HEALTH NEWS (Oct. 12, 2018), https://khn.org/morning-breakout/within-a-few-years-90-of-americans-of-european-descent-will-be-identifiable-from-DNA-through-genealogy-sites/.

2018, Yanic Erlich, former computational geneticist at Columbia University and the chief science officer of MyHeritage, another large DTC-GTC, conducted a research study using the MyHeritage database, which at the time contained 1.28 million DNA profiles, less than either Ancestry.com or 23andMe.[40] Erlich and his team concluded that if a person lives in the United States and is of European ancestry, there exists a 60% chance that a third cousin or closer relative has a genetic profile in the My Heritage database.[41] Moreover, 40% of individuals having Sub-Saharan or African descent would have a third cousin or closer in the database.[42] They did the same study using 30 random profiles using the GEDmatch database and their results were similar.[43] The geneticists concluded that in two or three years, 90 percent of Americans or European descent would be identifiable.[44]

Considering the number of people that now have used one of these DTC-GTCs,[45] odds are that there will soon be enough information in one of these databases to basically identify virtually any person in the United States through a distant relative.

II. GENETIC PRIVACY: REGULATION AND MANAGEMENT

a. Self-Regulation by DTC-GTCs

Self-regulation is in the best interest of the DTC-GTCs for numerous reasons. The more these businesses can successfully self-regulate, the less governmental oversight they will require. Self-regulation also apparently is encouraged by the government. "[T]he White House, Congress, and the Federal Trade Commission ("FTC") have encouraged private sector responses to privacy challenges in lieu of

40. Jocelyn Kaiser, *We Will Find You: DNA Search Used to Nab Golden State Killer Can Home in on About 60% of White Americans*, SCIENCE MAGAZINE (Oct. 11, 2018, 2:00 PM), https://www.sciencemag.org/news/2018/10/we-will-find-you-DNA-search-used-nab-golden-state-killer-can-home-about-60-white.

41. *Id.*

42. *Id.*

43. *Id.*

44. *Id.*

45. Matthew Haag, *FamilyTreeDNA Admits to Sharing Genetic Data With F.B.I.*, N.Y. TIMES (Feb. 4, 2019), https://www.nytimes.com/2019/02/04/business/family-tree-DNA-fbi.html; Company Facts, ANCESTRY, https://www.ancestry.com/corporate/about-ancestry/company-facts (last visited Aug. 29, 2019) (noting that Ancestry has tested the DNA of over fifteen million people). *See* also Antonio Regalado, *More Than 26 Million People Have Taken an at-Home Ancestry Test*, MIT TECHNOLOGY REV. (Feb. 11, 2019).

new regulation."[46] Additionally, successful self-regulation with respect to privacy issues will gain them more consumer trust.[47]

On July 31, 2018, the Future of Privacy Forum published the Privacy Best Practices for Consumer Genetic Testing Services.[48] In all, a group of DTC-GTCs (23andMe Inc., Ancestry, Helix, MyHeritage, and Habit) were involved publishing the Best Practices.[49] "[T]hese Best Practices include: (1) Transparency; (2) Consent; (3) Use and Onward Transfer; (4) Access, Integrity, Retention, and Deletion; (5) Accountability; (6) Security; (7) Privacy By Design; and (8) Consumer Education."[50]

The Best Practices recognize "that Genetic Data is sensitive information that warrants a high standard of privacy protection because of the following reasons: It may be used to identify predispositions, disease risk, and predict future medical conditions[;] It may reveal information about the individual's family members, including future children[;] It may contain unexpected information or information of which the full impact may not be understood at the time of collection[; and] It may have cultural significance for groups or individuals."[51] In addition, the Best Practices sets forth guidelines for dealing with law enforcement requests and states: "Genetic Data may be disclosed to law enforcement entities without Consumer consent when required by valid legal process."[52]

---

46. Joel R. Reidenberg et al., Disagreeable Privacy Policies: *Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 43 (2015), https://lawcat.berkeley.edu/record/1126239?ln=en.

47. As will be discussed in Section III b. *infra*, HIPAA and GINA already impact some of the services offered by DTC-GTCs and the FDA regulates what tests can be sold to consumers. Barbara J. Evans, *HIPAA's Individual Right of Access to Genomic Data: Reconciling Safety and Civil Rights*, 102 AM. J. HUM. GENETICS 5, 5–7 (Jan. 4, 2018), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5777935/pdf/main.pdf.

48. *Privacy Best Practices for Consumer Genetic Testing Services*, FUTURE OF PRIVACY FORUM (July 31, 2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf; *see Supporters*, FUTURE OF PRIVACY FORUM, https://fpf.org/about/supporters/ (last visited July 29, 2019) (Ancestry, 23andMe, and Helix, are listed as corporate supporters of the Future of Privacy Forum. There are many other major companies and law firms listed as well, including Amazon, Apple, Verizon, Uber, Google, Citigroup, Ropes and Gray and Covington and Burling, to name a few).

49. Carson Martinez, *Privacy Best Practices for Consumer Genetic Testing Services*, FUTURE OF PRIVACY FORUM (July 31, 2018), https://fpf.org/2018/07/31/privacy-best-practices-for-consumer-genetic-testing-services/?source=post_elevate_sequence_page.

50. *Privacy Best Practices for Consumer Genetic Testing Services*, FUTURE OF PRIVACY FORUM (July 31, 2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf.

51. *Id.*

52. *Id.*

Despite these articulated best practices, allowing DTC-GTCs to self-regulate simply may not be in the best interest of the consumer. Self-regulation certainly does not guarantee any consumer privacy. That became quite evident when FamilyTreeDNA entered into an agreement with the FBI to allow the government agency to test DNA samples in their database to obtain familial matches.[53] Even worse, by the time the company made the announcement, FamilyTreeDNA already had been sharing this information without prior notice to its customers.[54] Ironically, FamilyTreeDNA was an original signatory to the Privacy Best Practices for Consumer Genetic Testing Services, but after its announcement, was removed as a supporter.[55] It was the first time a DTC-GTC had voluntarily given "routine access to customer's data."[56] According to an op-ed piece published on The Future of Privacy Forum, "unfettered law enforcement access to genetic information on commercial services presents substantial privacy risks."[57]

FamilyTreeDNA's agreement is out of step with consumer expectations. Leading genetic testing companies understand that when users send in their DNA to learn more about their health or heritage, they do not expect their genetic data to become part of an FBI genetic lineup. FamilyTreeDNA users have not received a meaningful notice or opportunity to opt-in or opt-out of these searches. If this agreement remains in place and valid legal process is not obtained before access to genetic data is provided to the FBI, individuals may be erroneously swept up in investigations simply because their DNA was found near a crime scene or at a location where a victim or suspect lived or worked. Genetic profiles turned over to the FBI may also be covertly reused by the FBI on other commercial sites.[58]

This situation highlights the very reason why self- regulation alone, unfortunately, is not the solution. The reality is that there is

53. Kristen V. Brown & Bloomberg, *A Major DNA-Testing Company Is Sharing Some of Its Data With the FBI. Here's Where it Draws the Line*, FORTUNE (Feb. 1, 2019), https://fortune.com/2019/02/01/genetic-testing-consumer-DNA-familytreeDNA-fbi/.

54. Matthew Haag, *FamilyTreeDNA Admits to Sharing Genetic Data With F.B.I.*, N.Y. TIMES (Feb. 4, 2019), https://www.nytimes.com/2019/02/04/business/family-tree-DNA-fbi.html; John Verdi & Carson Martinez, *FamilyTreeDNA Agreement with FBI Creates Privacy Risks*, FUTURE OF PRIVACY FORUM (Feb. 6, 2019), https://fpf.org/2019/02/06/familytreeDNA-agreement-with-fbi-creates-privacy-risks/.

55. John Verdi & Carson Martinez, *FamilyTreeDNA Agreement with FBI Creates Privacy Risks*, FUTURE OF PRIVACY FORUM (Feb. 6, 2019), https://fpf.org/2019/02/06/familytreeDNA-agreement-with-fbi-creates-privacy-risks/.

56. *Id.*

57. *Id.*

58. *Id.*

nothing to prevent a DTC-GTC or a genealogy research cite from doing the exact same thing that FamilyTreeDNA did with its database. The current Privacy Best Practices also provides absolutely no real consumer protection from other companies that may obtain this information by, for example, a direct purchase of the DTC-GTC or a fourth party that is assisting in a law enforcement investigation. In 2018, pharmaceutical giant GlaxoSmithKline purchased a 300-million-dollar equity stake in 23andMe.[59]

Had they purchased 23andMe rather than just a share, there would be nothing binding them to adhere to the Privacy Best Practices as they relate to law enforcement uses. Disclosures by a pharmaceutical company like Glaxo would perhaps be under heavier scrutiny because of laws like GINA and HIPAA, but the same is not true for a non-pharmaceutical entity either in the United States or elsewhere. In addition, even though the European Union, through the General Data Protection Regulation ("the GDPR") has taken steps to protect the privacy of its citizens, the same is not true of companies in other countries where individual privacy is not paramount. Thus, while there surely may exist incentives for DTC-GTCs to protect the privacy of their consumers, other more compelling considerations, financial or otherwise, may prevail while a consumer's privacy takes a back seat.

b. Existing Governmental Regulations

Genetic privacy does have protection in certain situations related to the healthcare and insurance industries. There are three main areas that current laws, both state and federal, protect: (1) discrimination; (2) data security; and (3) regulation of genetic testing.[60] GINA and its state counterparts, protect individuals from discrimination by employers and insurance companies.[61] HIPAA protects genetic information in research and clinical settings, but it focuses on data security.[62]

59. Jamie Ducharme, *A Major Drug Company Now Has Access to 23andMe's Genetic Data. Should You Be Concerned?*, TIME (July 26, 2018), https://time.com/5349896/23andme-glaxosmith-kline/.

60. Rhys Dipshan, *Giving Away Your Genes: US Laws' Blind Spot With DNA Data*, LAW.COM (Aug. 2, 2018), https://advance.lexis.com/search?crid=C6873221-0efe-4b44-90fb-a0ccf1997e26&pdsearchterms=LNSDUID-ALM-AMLAWR-gmk45edgdi&pdbypasscitatordocs=False&pdmfid=1000516&pdisurlapi=true.

61. *Id.*

62. 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, 40 (2018); Dipshan, *supra* note 60.

HIPAA, however, only applies to certain entities and DTC-GTCs do not usually qualify.[63] If DTC-GTCs do not qualify, research sites like GEDmatch certainly do not either. The third and last category, regulations of genetic testing, are usually found in state laws.[64] Like GINA and HIPAA, these are laws that mostly govern in cases of insurance, employment and health care organizations.[65] For example, genetic testing laws in Alaska, Arizona, California, Delaware, Georgia, Iowa, Illinois, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, New York, Oklahoma and Rhode Island and South Carolina require a person's consent before their genetic data is disclosed.[66]

From the consumer protection perspective the Federal Trade Commission ("FTC") has the authority to investigate and prosecute DTC-GTCs for deceptive or unfair privacy policies or terms of use.[67] That being said, any deceptive or unfair privacy practices or terms of use have not been effectively used to protect users from law enforcement searches. When it comes to consumers using DTC-GTCs, none of these laws have provided protection to the innocent consumer from law enforcement's use of their genetic data to conduct familial DNA testing, particularly for those who purely are using the DTC-GTCs for ancestry purposes. Thus, there is no comprehensive regulation that protects the general privacy rights of consumers who use DTC-GTC or genetic ancestry research websites.[68]

c. Self-Management: A Heavy Burden Is On The Consumer

One of the arguments that can be made against exercising any sort of government control over privacy is the notion of "self-management." Self-management is defined as the privacy management of data by individuals and places the burden of navigating the complex world of online disclosure and consent squarely on the consumer.[69] Indeed it might be preferable to have individuals effectively self-man-

63. Hazel & Slobogin, *supra* note 62, at 40.
64. Dipshan, *supra* note 60.
65. *Id.*
66. *Id.*
67. *Id.*; *see* Hazel & Slobogin, *supra* note 62 at 41 ("The FDA has relatively broad authority to regulate DTC-GTCs but has thus far exercised "enforcement discretion," limiting its regulation to companies offering certain "health-related" genetic tests").
68. *Id.* at 40–41.
69. *See* Tuukka Lehtiniemi & Yki Kortesniemi, *Can the Obstacles to Privacy Self-Management be Overcome? Exploring the Consent Intermediary Approach*, BIG DATA & SOC'Y 1, 2 (July 2017), https://journals.sagepub.com/doi/pdf/10.1177/2053951717721935.

age their data. As with other areas of the law, over-regulation is not always the best way to solve a problem. There also are individuals who do not want the government trumping their ability to choose or decide issues that they may view as private. Still, in the world of online notices, consent and waivers, itself complex enough, the failure to understand the genetic privacy rights they are giving away may cause damage beyond what is superficially apparent.

The concept of self-management of data is not a new one. In an article entitled, "Privacy Self-Management and the Consent Dilemma," Daniel Solove discusses the origins of the term "self-management" as it relates to data privacy.[70] Solove addresses the issue of "paternalistic" law making to protect privacy versus the more hands off "libertarian" view and comes to the conclusion that a solution to the self-management dilemma should be a combination of the two.[71] That article, however, did not specifically address genetic privacy.[72]

While the privacy of all data is important, one's genetic data derived from testing merit additional protections that self-regulation using a hands-off approach simply may not be able to address. Moreover, the privacy of one's own genetic information is not the only privacy concern at stake. The privacy concern also belongs to the family members of that individual.

Given the muddy and sometimes convoluted notice provided to consumers on DTC-GTC websites, individuals may not consider the possibility that their genetic data may be used by law enforcement, could be sold to another company, or that a DTC-GTC could go bankrupt and have its assets and information sold, or that the company itself might change its rules and decide to sell the information they told the consumer it would not sell. Additionally, no one can predict what will happen in the future when it comes to scientific and technological breakthroughs and what scientists will be able to do or discover using someone's genetic code.

Can that information one day be used against you by a future employer? By a future insurer? By a genetics company? By a law enforcement agency?[73] Compounding this issue is the concern that,

70. *See* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1882 (2013), https://pdfs.semanticscholar.org/809c/bef85855e4c5333af40740fe532ac4b496d2.pdf.

71. *Id.* at 1901.

72. *See id.* at 1883.

73. *See GEDmatch.Com Terms of Service and Privacy Policy*, GEDMATCH (Dec. 9, 2019), https://www.gedmatch.com/tos.htm ("We cannot predict what the future holds for DNA or gene-

"[f]or their part, direct-to-consumer testing companies have been less than forthright about these dangers, usually burying privacy disclaimers deep in their contracts and refusing to disclose how long they keep customer data or how it can be used."[74] Research published by *Nature* found that DTC-GTCs "frequently fail to meet even basic international transparency standards."[75] Yet, consumers still are expected to "manage their privacy by weighing the subjective costs and benefits of data collection. In practice, however, many are neither well informed on the issues of their personal data or feel in control of it." Additionally, "[p]rivacy self-management has to take into account the highly divergent preferences people have on the desirable position along the secrecy-transparency spectrum."[76] There are "privacy *fundamentalists,* who have high privacy concerns, *pragmatists,* who have some concerns but favour individual choice, and the *unconcerned,* who have low concerns and tend to trust data collectors."[77] Additionally, a consumer's privacy is not static, and privacy decisions are dependent on context.[78]

In order to use a DTC-GTC, consumers make the privacy decision at the start of the process when they decide that they want to use the DTC-GTC, and this is when they are preliminarily expected to assess the "future harms and benefits."[79] The focus is on the immediate benefit of obtaining the testing.[80] Thus, "while immediate harms may be insignificant, long-term harms can develop gradually over time. Having to make the decision before the outcomes arise is arguably a feature of most human decision-making. However, with personal data, the timing poses particular difficulties due to the inherent dynamics arising from the data analysis technologies. As harms and benefits may arise by mechanisms which are not discernable, or do not yet even exist, the consequences of a disclosure are a moving target. Yet a consent, once given, is typically in effect indefinitely."[81] Addi-

alogy research. We cannot predict what the future will be for GEDmatch. It is possible that, in the future, GEDmatch will merge with, or operations will be transferred to other individuals or entities.").

74. Peter Pitts, *The Privacy Delusions of Genetic Testing*, FORBES (Feb. 15, 2017, 1:26 PM), https://www.forbes.com/sites/realspin/2017/02/15/the-privacy-delusions-of-genetic-testing/#3277de641bba.

75. Lehtiniemi & Kortesniemi, *supra* note 69, at 2.

76. *Id.*

77. *Id.*

78. *Id.*

79. *See* Solove, *supra* note 70, at 1890.

80. *Id. at 1891*

81. *See* Lehtiniemi & Kortesniemi, *supra* note 69, at 3.

tionally, research shows that there exist cognitive problems that hinder a person's ability to make informed choices about their data.[82] According to Solove, "people's actual ability to make such informed and rational decisions does not even come close to the vision contemplated by privacy self-management."[83]

One of the issues relates to the fact that consumers are not well-informed with the current click-wrap, "notice and choice" model that almost all online companies use. DTC-GTCs, much like every other internet company, uses the "notice and choice" model for disclosures.[84] According to the Notice and Choice Framework, notice must be provided so that the consumer can make a "Choice." The word "Choice" translates to the consumer consenting to whatever has been set forth in the Notice. "[A]t its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information—i.e., uses beyond those necessary to complete the contemplated transaction."[85]

There does not appear to be much difference between the Notice and Choice Framework used by DTC-GTCs and the Notice and Choice Framework used by other online providers of services. While the method is the same, the information it pertains to is not. The privacy of information such as date of birth, address, or gender, for example, cannot be compared to genetic information. Nonetheless, whether it is the purchase of software or providing DNA for a genetic test, the burden rests with the consumer either to accept the terms and notices, to walk away from the purchase or not use the service, or to purchase the item.[86] Thus, at the moment when consumers have psychologically committed to the purchase, they must either click through very lengthy notices or simply hit "I accept."[87] If the consumer does not accept all the terms and conditions, the consumer will not be able to complete the purchase of the test kit.

82. *See* Solove, *supra* note 70, at 1883.
83. *Id.*
84. *See* Reidenberg et al., *supra* note 46, at 43.
85. *Id.* at 44.
86. *See* Solove, *supra* note 70, at 1884.
87. It is no wonder that in one 2015 European poll, 18% of respondents said they read privacy policies fully and 49% only partially read them. https://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_431_sum_en.pdf.

d. Consent

The biggest privacy issue with the self-management of DTC-GTCs is therefore that of consent. The notion is that by agreeing to the terms and conditions of the DTC-GTCs, the consumers have provided consent, which may waive a variety of rights they may have had regarding the privacy of their genetic data. The problem with consent given in the typical click-wrap form is that genetic testing is not like other consumer products. If, for example, a consumer wants to add specialized testing, which is provided by 23andMe to test for Parkinson's, Alzheimer's, or BRCA1 and/or BRCA2, they must agree to *all* the terms at the commencement of the process or forego testing on that site. If someone else would like to use, for example, Ancestry.com to track down a long-lost relative, they too must do the same. That includes the acknowledgment that the police can access their genetic information.

Moreover, the problem is not just that consent is buried in the full panoply of disclosures. There is no consistency in how one consents to particular situations. For example, in the case of notice that law enforcement may have access to a consumer's genetic information, FamilyTreeDNA users are automatically opted in to allow law enforcement to see their profile.[88] Should they wish to not expose themselves to a law enforcement search, they would have to know to go to settings and opt out.[89] On the other hand, in May 2019, GEDmatch changed its policy, which was the same as FamilyTreeDNA's, and currently consumers must opt in to allow law enforcement to use their genetic profile.[90]

In the European Union, the GDPR has provided rules regarding valid consent. Article 7 states:

> "1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
>
> 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguisha-

88. *Law Enforcement Matching – Frequently Asked Questions*, FAMILY TREE DNA, https://www.familytreeDNA.com/learn/ftDNA/law-enforcement-faq/ (last visited Aug. 3, 2019).

89. *Id.*

90. Amy Docker Marcus, *Customers Handed Over Their DNA. The Company Let the FBI Take a Look,* WALL ST. J., Aug. 22, 2019, *available at* https://www.wsj.com/articles/customers-handed-over-their-dna-the-company-let-the-fbi-take-a-look-11566491162.

> ble from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
>
> 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.
>
> 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract."[91]

The GDPR does not directly address the law enforcement notice issues, but it does give guidance on how better to provide notice and obtain consent from DTC-GTC consumers. Its requirement in section 2 that consent must be clearly distinguishable when it pertains to different matters is a step in the right direction for making consent issues clearer to the consumer. For example, it also provides for a right to withdraw consent. Finally, section 4 addresses the problem of making services conditional on consent, something that occurs in DTC-GTCs, thereby calling into question the validity of the consent. Nonetheless, the GDPR still puts most of the burden on the consumer and does not address the impact to family members of the consumer.[92]

On the state level, some legislators also have begun to tackle the confusing consent notices used by DTC-GTCs. In early 2020, several representatives in the state of Washington introduced a bill that contains, *inter alia*, the following language:

> Sec. 2. (1) To safeguard the privacy, confidentiality, security, and integrity of a consumer's genetic data, a direct-to-consumer genetic testing company shall: (a) Provide clear and complete information regarding the company's policies and procedures for collection, use, or disclosure of genetic data by making available to a consumer: (i) A *high-level privacy policy overview* that includes basic, essential information about the company's collection, use, or disclosure of genetic data; and (ii) A *prominent, publicly available, and easy to*

91. *Art. 7 GDPR Conditions for Consent*, INTERSOFT CONSULTING, https://gdpr-info.eu/art-7-gdpr/ (last visited Aug. 3, 2019) (emphasis added).

92. Mark MacCarthy, *It's Time for a Uniform National Privacy Law*, CIO (Aug. 23, 2018, 11:49 AM), https://www.cio.com/article/3300106/it-s-time-for-a-uniform-national-privacy-law.html.

> *read privacy notice* that includes, at a minimum, information about the company's data collection, consent, use, access, disclosure, transfer, security, and retention and deletion practices; (emphasis added)[93]

Should this become law, it certainly would be a step in the right direction, but without more states following suit, there is little protection for the millions of other users.

e. Anonymity, Deidentification and Privacy

Contrary to what consumers may think, using DTC-GTC companies does not ensure anonymity. According to a 23andMe cofounder, Linda Avey, "it's a fallacy to think that genomic data can be fully anonymized."[94]

Even though DTC-GTCs say that they maintain anonymity of individuals and that they scrub the data so that it is "deidentified," the fact is that even the Privacy Guidelines themselves state that the deidentified information of individuals does not "strongly protect" them from reidentification: "Deidentification and Genetic Data: Deidentified information is not subject to the restrictions in this policy, provided that the deidentification measures taken establish strong assurance that the data is not identifiable. "We note that currently, *Genetic Data held at the individual-level that has been de-identified cannot be represented as strongly protecting individuals from re-identification, based upon existing deidentification tools and standards*. Such data may be protected in other ways and used for research with appropriate consent and security controls"[95]

Even if consumers do take the time to delve a little deeper into the methods used for de-identification or what that actually means for privacy, doing so would unlikely clarify the situation for them. In a footnote, the Privacy Guidelines cite the U.S. Department of Health & Human Services Guidance on Methods of Deidentification for HIPAA, which provides a rather complex set of procedures for any person to completely understand.[96] Thus, assuming that a consumer

93. 2020 Wash. Sess. Laws HB 2485.

94. *See* Pitts, *supra* note 74.

95. *See* Future Of Privacy Forum, *supra* note 48, at 5 (emphasis added).

96. *Id. at n. 18*; *see Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Aug. 3, 2019) (presenting guidance for the HIPAA Safe Harbor Method).

has even gone this far, without a genetics background, the U.S. Department of Health & Human Services Guidance is unlikely to shed any light on the issue. Providing the consumer with information about their efforts to maintain anonymity, if anything, gives consumers a false sense of security. Other sections of the notices in some DTC-GTCs support that idea.

For example, Paragraph 6 of 23andMe's Privacy Policy, entitled Security Measures, states: De-identification/Pseudonymization. Registration Information is stripped from Sensitive Information, including Genetic and Self-Reported Information. This data is then assigned a randomly generated ID so an individual cannot reasonably be identified.[97]

However, what is readily apparent is that law enforcement can and does get information that can be reidentified by someone, either within the DTC-GTCs or by some other party. For example, 23andMe's Privacy Statement states:

As required by law: Under certain circumstances your Personal Information may be subject to processing pursuant to laws, regulations, judicial or other government subpoenas, warrants, or orders. For example, we may be required to disclose Personal Information in coordination with regulatory authorities in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. *23andMe will preserve and disclose any and all information to law enforcement agencies or others if required to do so by law or in the good faith belief that such preservation or disclosure is reasonably necessary to: (a) comply with legal or regulatory process (such as a judicial proceeding, court order, or government inquiry) or obligations that 23andMe may owe pursuant to ethical and other professional rules, laws, and regulations*; (b) enforce the 23andMe Terms of Service and other policies; (c) respond to claims that any content violates the rights of third parties; or (d) protect the rights, property, or personal safety of 23andMe, its employees, its users, its clients, and the public. View our Transparency Report for more information.[98]

Much like the other large DTC-GTCs, 23andMe's Privacy Policy makes clear that 23andMe will abide by a subpoena, warrant, judicial proceeding, court order, or government inquiry and turn over information about the consumer if required to do so by law.

97. *Privacy Highlights*, 23ANDME (July 17, 2018), https://www.23andme.com/about/privacy/ (last visited September 9, 2019).

98. *Id.*

It also goes on to say, somewhat vaguely, that it will also turn the consumer's information over due to "obligations that 23andMe may owe pursuant to ethical and other professional rules, laws, and regulations."[99] It is unclear how broadly this part of the policy is applied by the DTC-GTC or what exact information they will provide.

Thus, de-identification of data does not mean that consumers have true anonymity when the data can be re-identified. Recent high publicity criminal cases prove that anonymity is not even a bump in the road when the police use third party familial DNA testing to find a suspect. The samples and results can be re-identified quite easily. More worrisome is the fact that with open source sites like GEDmatch they are an ". . . open source trove of potential leads, which, unlike forensic databases, contains genetic bits of code that can be tied to health data and other personally identifiable information."[100]

Additionally, GEDmatch's Terms of Service and Privacy Policy states, "GEDmatch exists to provide DNA and genealogy tools for comparison and research purposes. It is supported entirely by users, volunteers, and researchers. DNA and Genealogical research, by its very nature, requires the sharing of information. Because of that, users participating in this Site agree that their information will be shared with other users."[101]

Of course, it is fair to assume that to the average reader using this site, the other users are people like them, who are attempting to conduct DNA or genealogical research. It also is not clear what information is being shared.

Moreover, a consumer can upload not only their own raw DNA data, but they can upload the DNA of a person for whom they serve as guardian, the DNA of a person who has given the user authority to upload their data to GEDmatch, the DNA of a deceased person, [and] DNA that is "obtained and authorized by law enforcement to identify a perpetrator of a violent crime against another individual, where 'violent crime is defined as murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault."[102] Interestingly, by their

99. *Id.*

100. Megan Molteni, *The Future of Crime-Fighting is Family Tree Forensics*, WIRED (Dec. 26, 2018, 8:00 AM), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/.

101. *See* GEDmatch, *supra* note 73.

102. *Id.*

own definition, DNA from a "non-aggravated" rape case would not be authorized as raw data that can be submitted. How GEDmatch defines an aggravated rape is not stated.[103]

Their sentence construction also makes it appear that a robbery need not be "aggravated."[104] Perhaps it is using definitions from the company's state of incorporation or location, but given that it presumably works with law enforcement from around the country, such vague word usage merely adds to consumer confusion.

III. LAW ENFORCEMENT USE OF GENETIC DATA AND THE FOURTH AMENDMENT

a. Putting Away the "Bad Guys"

At the beginning of any genetic privacy discussion in the DTC-GTC and genealogical research arenas, it bears mentioning that there may be multiple stakeholders of that right. Among them are: (1) the consumer; (2) all of the members of the consumer's immediate and extended family, alive or not yet born who share the consumer's DNA profile (including the target of a law enforcement who may ultimately be charged with a crime); (3) the DTC-GTC company itself that may claim ownership rights as a result of their agreement with the consumer; (4) and any other company who may claim ownership rights, for example, via a purchase of any or all of the Data the DTC-GTC has.

At the heart of this discussion, however, is the original consumer and, for purposes of this article, the focus largely remains there. As in so many situations in which an individual's privacy right has been balanced against a concern for "safety," privacy rights sometimes have been ceded for the "greater good." In the world of criminal justice, unfortunately, it sometimes seems no price is too high for some as long as we "put away the bad guys," especially when the "bad guy" is someone who has committed numerous, heinous crimes like the Golden State Killer.

Those arguments might work better with something less intrusive, like fingerprints, but not one's genetic code. DNA is different. The genome that makes an individual unique and carries with it such private information is not like a fingerprint. As Supreme Court Justice Antonin Scalia astutely noted in *Arizona v. Hicks*, "there is nothing

103. *See* GEDmatch, *supra* note 73.
104. *Id.*

new in the realization that the Constitution sometimes insulates the criminality of a few in order to protect the privacy of us all."[105]

Of course, the compelling "greater good" arguments are not just restricted to "putting bad guys away." Some might argue that a future where everyone's genetic profile is in a centralized database would be safer for society. Others may argue that having everyone's DNA in one database would be more racially diverse than the existing CODIS database is.[106] Or, for example, when balancing privacy with the "greater good" of finding a cure for Alzheimer's, Parkinson's, or cancer, some would argue that individual genetic privacy should cede to medical advancements or cures for these diseases, and that genetic codes, even in DTC-GTC databases, should be used in that research.[107]

The arguments are no doubt compelling, but they do not overcome the magnitude of the societal invasion of privacy. No one can argue that catching criminals, especially those who have committed the most heinous of crimes, is not a valid interest. Moreover, no one would argue against finding a cure for deadly diseases. And indeed, a universal database may make society safer and it may be less racially biased than the CODIS database. However, a universal database would require the permanent relinquishment of every single person's most private information.

b. Law Enforcement's Use of DTC-GTCs

The serious nature of the relinquishment of genetic privacy cannot be overstated or, for that matter, easily understood by non-geneticists. Moreover, those genetic data privacy rights are that of not only the consumer, but the consumer's entire family. What is particularly concerning about genetic privacy is what we do not know about DNA and its future uses. The average person who has used these DTC-GTCs or genealogy websites most likely is not an expert on genetics. Even non-geneticists who happen to know a bit more about genetics than the average person cannot predict what the magnitude of their privacy violation may be in an evolving genetics world. Its potential uses, both for good and bad, and the permanent privacy concerns

105. Arizona v. Hicks, 107 S. Ct. 1149, 1155 (1987).

106. Kirsten Dedrickson, *Universal DNA Databases: A Way to Improve Privacy?*, 4 J.L. & BIOSCIENCES 637, 647 (2018).

107. This genetic data used in research may have more protections under GINA and HIPAA than other types of genetic data.

DNA and its data have are not easily graspable. The only certain thing we do know about DNA and genetic data is that we cannot comprehend or predict what advances in DNA we will be able to accomplish in the future. Thus, it makes sense that the average consumer may not have immediate concerns about something they cannot even fathom may occur. Herein lies the problem: consumers cannot fear what they cannot even foresee to be a danger or a threat.[108]

Familial DNA testing through DTC-GTCs is being used more and more by law enforcement, although it is unclear how many times they have done so.[109] Familial DNA testing is when a genetic profile is created from the DNA sample from a crime scene and then run through a database to determine whether another genetic profile or profiles in that database are similar to it. That match will then provide an investigative lead into determining who might be a relative of the potential suspect.

According to its Transparency Report, current as of February 14, 2020 23andMe has had 7 law enforcement requests for the data of 10 users and has not provided any data without the "prior explicit consent of the users.[110] Ancestry.com's 2019 Transparency Report states that in 2019 it received nine "valid" law enforcement requests for information and it provided information in six out of the nine.[111] Eight of the nine were requests for investigations for credit card misuse, fraud, and identity theft.[112] However, one request was for access to Ancestry's DNA database pursuant to a warrant. According to its Transparency report, Ancestry challenged the validity of that request on "jurisdictional grounds" and did not provide any information to the police.[113] In 2018 Ancestry.com received 10 requests, complied

108. During the writing of this article, I had more than a dozen informal conversations with friends, family and acquaintances curious about the topic of my article. Interestingly, nearly all of them had done some sort of DTC-GTC testing or were thinking about doing it. When I asked about whether they had concerns about privacy, each of them gave me similar responses. They all told me it was anonymous so they were not worried. None of them had read the entire notice and consent sections of the websites. One person told me she had nothing to hide. However, when asked about whether they had not given any thought to the potential future uses of their (and their family members' DNA) by some unknown third party, they had not.

109. Some DTC-GTCs publish transparency reports, but not all do. This is an entirely self-regulated reporting decision by a DTC-GTC. Additionally, it is unknown how many times, for example, a law enforcement agency has used a service like GEDmatch surreptitiously.

110. *See Transparency Report*, 23ANDME, https://www.23andme.com/transparency-report/ (last visited February 24, 2020).

111. *Id.*

112. *Ancestry 2019 Transparency Report,* ANCESTRY, https://www.ancestry.com/cs/transparency (Aug. 3, 2019).

113. *Id.*

with 7, and that all the requests were for investigations for credit card misuse, fraud, and identity theft.[114] It also states that it received no "valid" requests for genetic information and did not provide any genetic information to law enforcement in 2018.[115]

After much searching on FamilyTreeDNA's website for a Transparency Report, this statement was found in the seventh and final section of the FamilyTreeDNA Law Enforcement Guide: "FamilyTreeDNA is working on publishing an updated Transparency Report that contains details on all law enforcement requests for user information that we receive. This report will also be updated to include the number of forensic samples and files we have received."[116] It also states, "Unless we are legally barred from doing so, our policy for any request of additional user information is to notify users of the request and supply a copy of the request prior to disclosure. In the U.S., law enforcement officials may prohibit this disclosure by submitting a court order pursuant to 18 U.S.C. § 2705(b) or state statute signed by a judge. We will assess requests not to notify users from law enforcement outside the U.S. under applicable law. For all requests, we may also elect, in our sole discretion, not to notify the user if doing so would be considered counterproductive and if we are not legally permitted to do so."[117]

GEDmatch has publicly stated that approximately 50 law enforcement agencies or their representatives have submitted samples to GEDmatch and that approximately 150 cases have been submitted.[118] Another genetics laboratory that routinely works with law enforcement, Parabon Nanolabs, has stated that its work has yielded almost 36 arrests.[119] Whether or not there is overlap between these figures is unclear. The methodology used by law enforcement to generate leads through familial DNA testing and the creation of a genetic tree of suspects can vary. In some instances, investigators take DNA from a crime scene and send it to a genetic laboratory, like Parabon Nano-

114. *Id.*

115. *Id.*

116. *FamilyTreeDNA Law Enforcement Guide*, FAMILYTREEDNA, https://www.familytreeDNA.com/legal/law-enforcement-guide (last visited Aug. 3, 2019).

117. *Id.*

118. Amy Docker Marcus, *The FBI Came Calling. The DNA Firm Answered.*, WALL ST. J., Aug. 22, 2019.

119. Madison Pauly, *Police Are Increasingly Taking Advantage of Home DNA Tests. There Aren't Any Regulations to Stop It*, MOTHER JONES (Mar. 12, 2019), https://www.motherjones.com/crime-justice/2019/03/genetic-genealogy-law-enforcement-golden-state-killer-cece-moore/.

labs. They then create a DNA profile that is like one a consumer would get from a DTC-GTC like 23andMe or Ancestry. That profile can be uploaded to GEDmatch to see if there are matches.

There can be more than one match of relatives to the 9th degree.[120] Another example of how law enforcement can build a genetic family tree of suspects is illustrated by their collaboration with FamilyTreeDNA. In 2018, FamilyTreeDNA made headlines when it shared its DNA database with federal investigators without having notified its users.[121] Apparently, FamilyTreeDNA had allowed the FBI to search its database of consumer genetic profiles to solve cold murder and rape cases.[122] The arrangement between FamilyTreeDNA appears to have been the first DTC-GTC to provide information knowingly to the government without a subpoena or warrant.[123] When it finally did notify its customers, it informed them that the FBI would be able to access their database like any other user would.[124] However, the arrangement between the FBI and FamilyTreeDNA goes further than allowing the FBI full access to its database. Pursuant to the agreement, FamilyTreeDNA's genetic testing laboratory also creates data profiles from the FBI's DNA samples, which will then allow the FBI to use them to search other genealogy websites.[125] "The method is being used more and more by police departments around the country. In the process, they have called upon geneticists to assist them in creating forensic family trees in order to solve cases."[126]

Familial DNA testing is prohibited by the FBI and the Agency cannot run those searches through the Combined DNA Index System ("CODIS") or the National Combined DNA Index System ("NDIS"), which is part of CODIS, although familial DNA testing is allowed in certain states.[127] In Arkansas, California, Colorado, Florida, Michi-

120. *See* Megan Molteni, *The Future of Crime-Fighting is Family Tree Forensics*, WIRED (Dec. 26, 2018, 8:00 AM), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/.

121. Matthew Haag, *FamilyTreeDNA Admits to Sharing Genetic Data with F.B.I.*, N.Y. TIMES (Feb. 4, 2019), https://www.nytimes.com/2019/02/04/business/family-tree-DNA-fbi.html.

122. *Id.*

123. *Id.*

124. Press Release: Connecting Families and Saving Lives, FAMILYTREEDNA (Feb. 1, 2019), https://blog.familytreeDNA.com/press-release-connecting-families-and-saving-lives/.

125. *Id.*

126. *See* MOLTENI, *supra* note 120.

127. *See Frequently Asked Questions on CODIS and NDIS*, FBI, https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet (last visited Aug. 8, 2019) ("Are familial searches performed at NDIS? No, familial searching is not currently performed at NDIS); *see also* 73 Fed.Reg. 74937 (Dec.10, 2008); *see also* Lauren Keiper, *More U.S. States Use Familial DNA as Forensic Tool*, REUTERS (Mar. 30, 2011, 8:38 PM), https://www.reuters.com/

gan, Texas, Utah, Virginia, Wisconsin, and Wyoming, familial DNA testing is legal and authorized for searches in CODIS/NDIS.[128] Maryland and Washington DC expressly prohibit familial searches done in CODIS/NDIS.[129] Additionally, on January 22, 2019, Maryland's House Judiciary Committee held a hearing on House Bill 30, introduced by Maryland State Senator Charles Sydnor III. House Bill 30 sought to amend Maryland's statute prohibiting familial DNA testing in the CODIS/NDIS database. The amendment to the statute would read: "A person may not perform a search of the statewide DNA database *OR ANY OTHER DNA OR GENEALOGICAL DATA BASE* for the purpose of identification of an offender in connection with a crime for which the offender may be a biological relative of the individual from whom the DNA sample was acquired." (caps original, emphasis added). That bill failed, and in February 2020, another bill was introduced again attempting to regulate various types of genetic database searches[130]

Other state legislators have been attempting to address the concerns about familial DNA testing. A Utah State Representative has introduced a bill that would limit the use by police of genetic databases for familial matches and the submission of genetic information to a genetic genealogy service. The Bill also would prohibit the police from entering false information or making a false representation to a genetic testing company or a genetic genealogy company.[131]

The familial DNA matching process has been done through CODIS and its related databases. The samples in those databases are samples that have been submitted of individuals processed through either a state or federal criminal justice system. That stands in stark contrast to law enforcement's use of GEDmatch, an open source gen-

article/us-crime-DNA-familial-idUSTRE72T2QS20110331 (allowed in Colorado, California, and Virginia, and under consideration in Pennsylvania).

128. FBI, *supra* note 124.[125] https://www.fbi.gov/services/laboratory/biometric-analysis/codis/codis-and-ndis-fact-sheet

129. *See* Avi Selk, *The Ingenious and 'Dystopian' DNA Technique Police Used to Hunt the 'Golden State Killer' Suspect*, THE SALT LAKE TRIBUNE (Apr. 28, 2018), https://www.sltrib.com/news/nation-world/2018/04/28/the-ingenious-and-dystopian-DNA-technique-police-used-to-hunt-the-golden-state-killer-suspect/ ("Familial DNA searches, in fact, had an 83 percent failure rate in a 2014 British study, Wired wrote. This is part of the reason that many warn against the practice, even as law enforcement agencies master its uses.").

130. DNA Databases Are Boon to Police But Menace to Privacy, Critics Say, THE PEW CHARITABLE TRUSTS, https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/20/dna-databases-are-boon-to-police-but-menace-to-privacy-critics-say (last visited Feb. 26, 2020)., http://mgaleg.maryland.gov/2020RS/bills/sb/sb0848F.pdf

131. *Id.*

ealogical research website, MyHeritage.com, 23andMe, Ancestry.com, and other DTC-GTCs like them where *innocent* citizens are submitting their DNA for reasons entirely personal to them. Thus, the important difference between familial DNA testing in the CODIS database and the use of DTC-GTCs is that the collection of samples submitted through CODIS are not only regulated and restricted, but they are of individuals who have been arrested and/or convicted of crimes. In stark contrast, law enforcement is now able to scour private DNA databases that contain the DNA of entirely innocent individuals. With the introduction of DTC-GTCs without any effective controls on the use of that DNA, the threat of use by law enforcement raises even more concerns. With their ever-growing database of DNA profiles, DTC-GTCs and "open source" genealogy websites like GEDmatch have become of great interest and use to law enforcement agencies, with or without the permission of the customers.[132]

The big-picture view of the future of DNA and its uses is a complex one. The use of DNA testing in criminal cases always has been a double-edged sword. DNA testing has proven to be an extraordinary tool in proving people's innocence. The strides made in the Innocence Movement would not have been possible without DNA testing. Moreover, as more samples are obtained from those arrested, the CODIS database grows and allows law enforcement to use those samples for comparison. Thus, there exists an uncomfortable relationship between the increase in exonerations through DNA testing and the growth and growing use of databases. One could not exist without the other. However, the CODIS database apparently has not sufficed. Law enforcement has, with increasing frequency, turned to DTC-GTC and other genealogy databases to solve cases. It is important to note that the CODIS database and the private genealogy databases differ in that, "[g]enetic genealogy . . . is drawn from hundreds of thousands of genetic variants called SNPs (for single nucleotide polymorphisms). The technique can give away details about a person's appearance, medical conditions and possibly even predisposition to mental health problems."[133] At least one journalist has referred to the ever-growing

132. MOLTENI *supra* note 120. The use of websites like GEDmatch currently do not require court orders

133. Tina Hesman Saey, *Genealogy Companies Could Struggle to Keep Clients' Data from Police,* SCIENCE NEWS (June 10, 2019, 12:00 pm), https://www.sciencenews.org/article/forensic-genetic-genealogy-companies-police-privacy

private genetic databases as the soon-to-be *de facto* national database[134]

Recently, the Golden State Killer of California was identified as Joseph DeAngelo and captured using familial DNA testing through GEDmatch.[135] The police uploaded a fake profile using the DNA from the case.[136] Between 1976 and 1986, the Golden State killer had killed 12 people and raped 45 women.[137] One of DeAngelo's distant relatives had uploaded their profile into the GEDmatch database and police were able to get a partial match to the genetic evidence they had uploaded with the fake profile they created.[138] Law enforcement does not actually need court approval to use GEDmatch or, for that matter, any other genetic database.[139] Moreover, there is very little that currently can be done to prevent them from creating false profiles and submitting samples in that manner.

In 2019, GEDmatch violated its own policy by restricting exactly which types of cases it would grant police permission to search its database for when it allowed Utah police to search its database in an aggravated assault and burglary case. Police submitted the DNA profile and matched it to a 17- year-old's great uncle. The 17- year- old was subsequently arrested and charged with aggravated assault and burglary.[140]

c. The Fourth Amendment and the Innocent Citizen

Privacy is at the heart of the Fourth Amendment. The Founding Fathers went to great lengths to protect citizens from governmental intrusion and Fourth Amendment jurisprudence has been evolving for

134. Natalie Ram, *The U.S. May Soon Have a De Facto National DNA Database*, SLATE (Mar. 19, 2019), https://slate.com/technology/2019/03/national-DNA-database-law-enforcement-genetic-genealogy.html.

135. SELK, *supra* note 129.

136. Sarah Zhang, *How a Tiny Website Became the Police's Go-To Genealogy Database*, THE ATLANTIC (June 1, 2018), https://www.theatlantic.com/science/archive/2018/06/gedmatch-police-genealogy-database/561695/.

137. Avi Selk, *The ingenious and 'dystopian' DNA Technique Police Used to Hunt the 'Golden State Killer' suspect*, THE SALT LAKE TRIBUNE (Apr. 28, 2018), https://www.sltrib.com/news/nation-world/2018/04/28/the-ingenious-and-dystopian-dna-technique-police-used-to-hunt-the-golden-state-killer-suspect/.

138. *Id.*

139. Megan Molteni, *The Future of Crime-Fighting is Family Tree Forensics*, WIRED (Dec. 26, 2018, 8:00 AM), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/.

140. Terry Spencer, *Use of Online DNA Databases by Law Enforcement Leads to Backlash and Website Changes*, PBS (June 7, 2019), https://www.pbs.org/newshour/nation/use-of-online-dna-databases-by-law-enforcement-leads-to-backlash-and-website-changes.

hundreds of years since then. In the context of law enforcement's use of DTC-GTCs, modern Fourth Amendment jurisprudence must grapple with a very basic question: does the Fourth Amendment offer any protection to the millions of innocent individuals who use these genetic databases?[141] In the past, scholars have argued for an Innocence Model of Fourth Amendment jurisprudence.[142] Others have maintained that the innocent are irrelevant to Fourth Amendment jurisprudence. And while remedies for privacy violations exist in tort and civil rights actions,[143] those remedies, when offered for a violation of the privacy right stemming from genetic material, submitted for one's own personal use, do not, and cannot, undo the irrevocable damage that occurs when a person's genetic information is obtained and used by law enforcement and other entities merely to create a potential suspect family tree.

Historically, Fourth Amendment concerns were not exclusively about criminal cases and exclusion of evidence at criminal trials, but also were about civil actions brought by citizens.[144] According to Professor Akil Reed Amar, the Fourth Amendment did not at the onset require exclusion of evidence in criminal cases, but rather it presupposed civil trespass suits.[145] "The 'right of the people to be secure in their persons, houses, papers, and effects' presupposes and conjures up tort law, which protects persons and property from unreasonable invasions. Here too, textual analysis is strongly supported by history-no framer ever argued for exclusion, nor did any early commentator, or judge-and by common sense: unlike tort law, exclusion rewards the guilty but gives absolutely zilch to the innocent citizen, whom the government seeks to hassle."[146] Thus, Amar argued, warrants were

141. Sherry F. Colb, *Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1457, 1461 (1996) https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1813&context=facpub. *See also* Tonja Jacobi and Ross Berlin, *Supreme Irrelevance: The Court's Abdication in Criminal Procedure Jurisprudence*, 51 UNIV. OF CAL. DAVIS 2033, 2038 (2018).

142. Sherry F. Colb, *Innocence, Privacy, and Targeting in Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1457, 1463 (1996) https://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=1813&context=facpub.

143. Peter Swire, *Professor Peter Swire Testimony in Irish High Court Case—Chapter 7: Individual Remedies in US Privacy Law*, ALSTON & BIRD (last visited Aug. 3, 2019), https://www.alston.com/-/media/files/insights//peter-swire-testimony-documents/chapter-7—individual-remedies-in-us-privacy-law.pdf?la=en.

144. Akhil R. Amar, *The Fourth Amendment, Boston, and the Writs of* Assistance, 30 SUFFOLK U. L. REV. 53, 64 (1996–97), https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1950&context=fss_papers.

145. *Id.*

146. *Id.*

meant to immunize the government from tort claims.[147] Nonetheless, the trajectory of Fourth Amendment jurisprudence moved from the more general privacy focus over the course of several hundred years to one that is almost purely focused on exclusion of evidence at trial.[148]

Thus, modern Fourth Amendment jurisprudence seems ill-prepared to handle the collapse of genetic privacy rights that may come with an unregulated genetic information world. It is fair to assume that as private genetic databases grow, law enforcement will turn to those databases with much greater frequency to solve crimes. On many of these sites, innocent citizens who would like to obtain genetic testing or to do genealogy research are left without a choice but to "consent" to allowing law enforcement to rummage through, and possibly use, their genetic data or they must forgo testing altogether on the vast majority of DTC-GTCs.

Many legal arguments made in support of allowing law enforcement to obtain and test these genetic samples have focused upon that Third-Party Doctrine, which is premised on the notion that information voluntarily provided to a third party vitiates any privacy claim one may have and that no warrant is needed by the police in order to obtain that information.[149] In *Carpenter v. United States*, however, the Supreme Court restricted the use of the Third Party Doctrine and held that the police need warrants to obtain historical cell-site location information about a person's whereabouts from a third party.[150] Justice Roberts, writing for the majority, observed that there have been "seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years."[151] Part of the reasoning included consideration of the fact that these records provide so much information about their users for so long.[152]

The rationale in *Carpenter* can be applied to genetic data because of its nature and because it belongs not only to the consumer, but to everyone who shares that consumer's genetic information. Genetic

147. *Id.* at 60.
148. *Id.* at 64.
149. John Villasenor, *What You Need to Know About the Third-Party Doctrine*, THE ATLANTIC (Dec. 30, 2013), https://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/.
150. Carpenter v. United States, 138 S. Ct. 2206, 2207 (2018).
151. *Id.* at 2219.
152. *Id.* at 2217.

data is not like a bank record, a telephone record, or even cell-site location data.[153] The content of those records does not reveal such personal information to the same extent. Genetic data can provide information about genetic familial markers, conditions, and other incredibly private details about an individual and their family members.

Additionally, there is support for the argument for greater genetic privacy protection in *Carpenter*'s dissenting opinions. Justice Kennedy dissented in *Carpenter* because he determined that Carpenter did not have ownership rights or control over the cell-site locations records and therefore had no expectation of privacy at all. Justice Gorsuch dissented stating that he would do away with the reasonable expectation of privacy test (as would Justice Thomas) and the third-party doctrine in favor of focusing on whether someone has some sort of property rights in the information. In contrast to the *Carpenter* facts, consumers who use DTC-GTCs do maintain some property rights. If consumers have the right to request that their information be deleted and that their samples be destroyed, they maintain control and ownership to some degree of their genetic data.

The genetic data housed at DTC-GTCs or other genealogy websites ought to be protected by, the Fourth Amendment. Law enforcement should be prohibited from conducting the genetic, modern-day equivalent of a search pursuant to a writ of assistance.[154] These are nothing more than genetic dragnet searches when the sole purpose of going through these databases is to find possible familial DNA matches in a case where there is no other clue as to who the suspect is. Without such a prohibition, there is no protection. Justice Scalia said, "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 law-enforcement searches. The Fourth Amendment must prevail."[155]

While concerns of genetic privacy pervade other areas such as health care and consumer protection, the constitutional privacy right against unreasonable searches and seizures is of the utmost concern, particularly because the intrusion also affects unknowing family mem-

153. *See* United States v. Miller, 425 U.S. 435 (1976) (holding no expectation of privacy for bank records); *see also* Smith v. Maryland, 442 U.S. 735 (1979) (holding records of telephone calls have no expectation of privacy).

154. See Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 501–512 (1995) (detailing history of American search and seizure case law).

155. *Id.*

bers separated by as many as nine degrees.[156] These privacy infractions are a world apart from those the courts historically were accustomed to dealing with during searches by the government. Such searches usually occurred at a moment in time. If there is an unlawful search of a home, it may be intrusive at that time, but it also is somewhat final and finite. In contrast, the privacy concern with genetic materials is more permanent and irreversible and as such cannot be viewed through the same lens. This rings especially true when the net is cast so wide as to include the genetic information of millions of completely innocent individuals use DTC-GTCs or genealogy research websites, which information may then be shared with 4th party providers in order to build a genetic family suspect tree.

If and when the police do seek a warrant, courts also must act as vigilant gatekeepers of our privacy rights in these types of cases.[157] There exist serious issues regarding whether or not search warrants affecting the privacy rights of millions of people ought to be issued for these types of database searches when the sole purpose is to obtain a familial match using the DNA of an innocent citizen. A search warrant requires probable cause, i.e. a fair probability that a search will result in evidence of a crime being discovered.[158] Search warrants also require specificity and particularity. For these reasons, the validity of these search warrant applications should not be a foregone conclusion. A warrant application for a search of a DTC-GTC or a genealogy research database is no more than a fishing expedition that also engages in a fair amount of bootstrapping. The only information law enforcement might possibly obtain is that of an innocent distant relative of an unknown suspect, assuming of course that the police have not established with probable cause that the suspect's own genetic profile is in the database. Depending on when in the process the police seek a warrant, it is only a possibility that an unknown suspect's family member will have submitted a sample to that database. It is entirely speculative. Even if the application for a search warrant occurs at some point after they have submitted a sample to the database, the sample matched in the DTC-GTC alone will not directly identify the suspect. It is only by bootstrapping the information derived from

156. *See* Megan Molteni, *The Future of Crime-Fighting is Family Tree Forensics*, WIRED (Dec. 26, 2018, 8:00 AM), https://www.wired.com/story/the-future-of-crime-fighting-is-family-tree-forensics/.

157. Nothing short of a search warrant should be utilized to obtain evidence from DTC-GTCs or a genealogical website.

158. Illinois v. Gates, 103 S. Ct. 2317, 2320 (1983).

the DTC-GTC to a second, yet-to-be done testing process, like the service provided by fourth party providers such as Parabon NanoLabs, genealogy researchers, or hobbyists, that police can link any possible family members with an actual suspect. Even then, law enforcement only can build a genetic family tree of suspects. Thus, it is too attenuated, should not establish probable cause, and the judiciary should exercise extreme caution and restraint in issuing such search warrants for these types of cases.

At least one court has not taken this cautious approach. In December 2019, the New York Times reported that a Florida detective announced at a police convention that he had obtained a warrant from a Florida judge to search the entire GedMatch database containing 1.2 million genetic profiles. What is especially troubling about the warrant is that the judge's order allowed the detective to override the privacy settings that were selected by users on Gedmatch. Of the 1.2 million Gedmatch users, in fact only 185,000 of the 1.2 million of the users, roughly 15%, had opted-in to allow law enforcement to view their genetic profiles.[159] Thus, approximately 1,015,000 people were subjected to non-consensual searches. Interestingly, that very same month that the court approved the Gedmatch search, Gedmatch was acquired by Verogen, Inc., a company that according to its website, was created exclusively to be a forensics genomic lab. It states, "Working in partnership with the community, we can elevate the forensic genomics lab's role in preserving public safety—and improve global justice for all."[160] Verogen is a company that already has ties to law enforcement in that Verogen's next-gen DNA technology has been approved by the FBI for upload to the National DNA Index System or NDIS. NDIS allows for DNA comparison of profiles submitted by both federal, state laboratories.[161]

CONCLUSION

Until there is consensus about the unique nature of genetic samples and data and its potential for revealing the most private confidential information about an individual, there can be no easy solution to

159. Kashmir Hill & Heather Murphy, *Your DNA Profile is Private? A Florida Judge Just Said Otherwise,* N.Y. TIMES (2019), https://www.nytimes.com/2019/11/05/business/dna-database-search-warrant.html (last visited Feb. 28, 2020).

160. Company, VEROGEN, https://verogen.com/company/ (last visited Feb 28, 2020).

161. FBI Approves Verogen's Next-Gen Forensic DNA Technology for National DNA Index System (NDIS), VEROGEN (2019), https://verogen.com/ndis-approval-of-miseq-fgx/ (last visited Feb 28, 2020).

genetic privacy. The genetic privacy of consumers who use DTC-GTCs should not be treated like other consumer data privacy. Because of the extremely sensitive and unique information about a person's genome, genetic data simply cannot be viewed in the same light as other data, digital or otherwise.

Nothing short of a complete ban by Congress on law enforcement's use of DTC-GTCs or ban on DTC-GTCs and other genealogical databases sharing such information with law enforcement will protect consumers, and society in general. Congress could create a national data privacy law, much like EU has done with the GDPR, or a free-standing genetic privacy law that prohibits familial DNA searches of any genealogical database. The same can be said of state legislatures. A hard and clear line must be drawn on the privacy of an *innocent* individual's DNA information that is contained in a DTC-GTC or genealogical database. To do less would be to take another step on the already slippery slope, which will inevitably lead to a complete loss of privacy for not only the person who used the DTC-GTC, but for that person's entire family.

If federal law enforcement agencies such as the FBI cannot, and do not, employ familial DNA testing using CODIS, which only houses the DNA of certain arrestees and convicted criminals, it makes absolutely no sense to allow them and other state or local law enforcement agencies to conduct those very same searches of innocent citizens through a back door.[162] Current use of DTC-GTCs amounts to a genetic fishing expedition, especially now as consumers play catch-up on the importance of protecting their genetic privacy. Such fishing expeditions violate the constitutional privacy rights of innocent citizens and their families. As DTC-GTCs databases grow larger, law-enforcement's appetite for using DTC-GTCs will grow along with them and could lead to an unregulated genetic surveillance state. What may have started as an interest in solving serious homicide cold cases, like that of the Golden State Killer, has already pivoted into a first line of defense for solving any and all crimes.[163]

162. Natalie Ram, *The U.S. May Soon Have a De Facto National DNA Database*, SLATE (Mar. 19, 2019), https://slate.com/technology/2019/03/national-dna-database-law-enforcement-genetic-genealogy.html.

163. *See* Natalie Ram, *The Genealogy Site That Helped Catch the Golden State Killer is Grappling With Privacy*, SLATE (May 29, 2019), https://slate.com/technology/2019/05/gedmatch-dna-privacy-update-law-enforcement-genetic-geneology-searches.html.

At the moment, there really is nothing in the way of DTC-GTCs deciding to allow the government to utilize their databases to conduct DNA searches for any and all crimes. For this reason, a genetic privacy law considered by Congress or the states should include a ban on the use of DTC-GTCs by law enforcement to conduct familial DNA testing. Whether or not they are inclined to do so remains to be seen. Perhaps the GEDmatch already has violated its own Terms and Policies when it permitted law enforcement to investigate an aggravated assault instead of the stated policy that is restricted to homicides, sexual assaults and abductions.

Passing such a blanket law seems unlikely, despite the necessity for such a hard line. Congress did not act when law enforcement continued to collect historical cell-site data. Rather, it took a decision from the Supreme Court in *Carpenter* to hold such warrantless searches unconstitutional. Given that congressional leaders may not want to appear "soft" on crime, it does not seem likely that they will want to ban familial DNA testing completely.

Absent Congressional or state action, there are other measures, admittedly only stop-gap in nature, that can be taken. First, all courts should acknowledge and consider the serious consequences of allowing such practices to continue absent strict limits. The Fourth Amendment's privacy right must be jealously guarded in order to insure the privacy of innocent citizens. The Third- Party Doctrine should not be applied and nothing short of a search warrant should be used to gain access to genetic information from a DTC-GTC or any other genealogical database. In that regard, courts should strictly adhere to the probable cause and specificity and particularity requirements, and not issue search warrants in cases such as these where law enforcement merely seeks to conduct a fishing expedition in a genetic database in the hopes of building their genetic suspect tree.

Additionally, even though at least one court was willing to completely ignore the privacy of over a million consumers, all genetic databases should be required to adopt an express opt-in model like the one adopted by GEDmatch. Otherwise, consumers have no choice, but to accept the Notice and Choice model generally used on DTC-GTCs websites if they seek to use the genetic testing company. These notices and terms are unnecessarily complex and convoluted and as such, any blanket type of user consent should not be construed as a voluntary waiver of any rights to be free of searches by law enforcement. Further, innocent citizens should not have to automati-

cally consent to the possibility of the police using their DNA in order to use a DTC-GTC, thus any notice of consent without more should not be deemed a waiver that allows police use. That consent also should not be part of a long laundry list of notices, buried in a myriad of other notices, but rather in a separate and distinct format. In that opt-in notice, transparency about the process and consequences of their consent should be required as well. Thus, the opt-in notice should explain, among other things, that by consenting to this use, their genetic profile and that of their immediate and extended family members, including the unborn, may be shared with additional parties other than law enforcement, such as third party geneticists, or ancestry volunteers and that their DNA data may possibly be entered into other unregulated websites and databases. It also should inform the consumer that while the use of their DNA may assist in catching a perpetrator of a crime, it also may implicate other family members who are innocent. It should state that any privacy rights that the consumer may have had with the DTC-GTC may not apply. Finally, it should inform the consumer that future unforeseen and unknown use of their genetic data by unknown companies or individuals is possible.

In conclusion, we, as a society, are at a crossroads. Congress, State legislatures, and all courts are at a crossroads. The concern about genetic privacy goes beyond the already significant general data privacy rights of the consumer. Do citizens want to live in a genetic surveillance state? Our Founding Fathers could not have imagined a world where the advances of science could identify a person on the genetic level. Justice Scalia, in his scathing dissent in *Maryland v. King*, aptly warned of a genetic panopticon. His warning applies even more to the government's use of the genetic information of private citizens and the concern that we are becoming a genetic surveillance state. Privacy is something that was then, and is now, recognized as a fundamental right in the United States. And genetic privacy ought to be considered sacred.