Direct-to-Consumer Genetic Testing: Maintenance of Individual Privacy

By: Jessica L Missel

Table of Contents

I. Introduction

Direct-to-Consumer ("DTC") genetic testing raises a set of concerns involving inadequate safeguards of test results to protect against the potential negative impact on personal privacy. The concerns arise from insufficient federal and state laws. In a technology-driven society, the prospect of data breaches releasing highly sensitive genetic information requires greater governmental oversight. This article explores the question of whether DTC genetic testing, specifically testing companies, should be subject to privacy requirements. An assessment of this issue requires first, an explanation of DNA testing technology, second, an analysis of the current privacy frameworks applicable to genetic testing, third, an assessment of the gaps in these frameworks, and last, consideration of mechanisms to maintain individual autonomy and privacy.

II. DNA Testing Technology

A "genetic test" is defined as "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes."[1] The evaluation of DNA testing technology begins with a brief description of the molecular analysis techniques followed by an in-depth analysis of DTC genetic tests ("DTC-GT") and genetic testing companies.

[1] 74 Fed. Reg. 51701.

A. Science of Genetic Testing

Genetic testing may be useful for determining paternity, matching forensic tissue, assessing ancestry, and identifying genetic predispositions to specific diseases or reproductive risks. DTC tests designed to identify genealogy or predisposition to disease are done by molecular techniques such as polymerase chain reaction ("PCR"), and next-generation sequencing (either whole-exome or whole-genome sequencing).[2]

1. The DNA Molecule

The Human Genome Project, started by the National Institute of Health ("NIH") in 1990, was designed to "decipher the massive amount of information contained in our genome – the DNA (deoxyribonucleic acid) found within all our chromosomes."[3] DNA is the molecule of life that makes up the chemical subunits of human chromosomes.[4] A gene is the unit of heredity passed from parent to offspring that affects traits/characteristics of an individual.[5] The primary purpose of DNA is to encode the information necessary in proteins for cell structure and function.[6] A cell synthesizes the proteins by a process known as gene expression in which a gene sequence affects the characteristics of the cell.[7] An individual's gene sequence leads to the expression of morphological, physiological, and behavioral traits.[8] An alternate version of a specific gene known as an allele can account for the differences in traits as each allele encodes a particular protein

[2] ROBERT J. BROOKER, GENETICS ANALYSIS & PRINCIPLES 616 (5th ed. 2015). [hereinafter Genetic Analysis].
[3] *Id.* at 1.
[4] *Id*. at 2.
[5] *Id.* at 4.
[6] *Id.* at 5.
[7] *Id.* at 6.
[8] *Id*. at 6-7.

function or expression.[9] These inherited differences in characteristics due to genetic variation[10] make genetic tests useful.

2. Polymerase Chain Reaction ("PCR") Testing

Molecular markers[11] are useful in polymerase chain reactions and gel electrophoresis.[12] PCR amplifies the gene from a sample of cells by separating the DNA strands with high temperature leaving two free single-stranded DNA molecules.[13] As the temperature lowers, primers made of short single-stranded DNA bind to specific sites in the template DNA, each binding near one end of the gene of interest.[14] Once the primers bind, the temperature is raised slightly, and a polymerase enzyme is added to the reaction to synthesize a strand of DNA complementary to the single-stranded template DNA.[15] The third step, known as primer extension results in double the amount of template DNA.[16] The three-step process of PCR can be repeated for as many cycles as necessary. A typical PCR run can take a couple of hours.[17]

Once the template DNA sequence has been amplified, it may be tested for the presence of the sequence by running either (1) the sample on a gel stained with ethidium bromide and observing if the gel fluoresces under UV light or (2) with real-time PCR.[18] Scientists can determine the amount of the specific product as the PCR runs by adding a probe that emits fluorescence at a particular wavelength.[19] If a fluorescent band of the correct size or the level of the fluorescence

[9] *Id*. at 7.
[10] *Id*. at 186.
[11] A molecular marker is a segment of DNA at a specific site along a chromosome. The markers may vary among individuals. Geneticists use the markers as references to determine patterns of genetic variations. *See id*. at 557t.
[12] *Id*. at 506.
[13] *Id*. at 505, 616.
[14] *Id*.
[15] *Id*. at 506.
[16] *Id*.
[17] *Id*.
[18] *Id*.
[19] *Id*.

from the probe increases, it indicates a successful amplification.[20] However, even with multiple PCR amplification cycles, next-generation sequencing continues to be the preferred method of genetic analysis because it can detect all variants and mutations.

3. Next-Generation Sequencing ("NGS")

Genotyping deals with differences in an individual's genetic makeup compared to another individual and looks at genetic variation among populations.[21] Whole-exome and whole-genome sequencing (next-generation sequencing) involves sequencing the individual's entire DNA as opposed to a gene of interest in PCR testing. Whole-exome sequencing examines the exons within the gene.[22] Exons are a portion of the genome that provides instructions for making proteins.[23] Whole-exome sequencing identifies variations in the protein-coding region of any gene, which is efficient in identifying possible disease-causing mutations.[24] However, whole-exome sequencing misses DNA variations that occur outside the exons but still affect gene activity.[25] Whole-genome sequencing can detect differences in any part of the genome and determines the order of all the nucleotides in an individual's DNA.[26]

4. Single Nucleotide Polymorphisms ("SNPs")

An even cheaper approach to DNA sequencing is to examine SNPs. A SNP is a site in the genome where one of the nucleotide bases (A, T, G, or C) occurs in several different forms among different individuals.[27] The common sites on the genome are used in the mapping of genes and

---

[20] *Id.*
[21] *Id.*
[22] DEP'T. OF HEALTH & HUMAN SERVS. NAT'L INST. OF HEALTH, NAT'L CTR. FOR BIOMEDICAL COMMC'N, HELP ME UNDERSTAND GENETICS: GENETIC TESTING (2019), https://ghr.nlm.nih.gov/ [hereinafter Genetic Testing].
[23] Genetic Testing, *supra* note 22, § Next-Generation Sequencing.
[24] *Id.*
[25] *Id.*
[26] *Id.*
[27] Genetic Analysis, *supra* note 2, at 557t.

disease-causing alleles during genetic testing as they involve a large number of variations.[28] Scientists use SNPs to estimate a person's ethnic background for ancestry tests and have identified more than one million SNPs, which correspond to clinical and non-clinical traits.[29]

B. What is a Direct-to-Consumer ("DTC") Genetic Test?

DTC genetic testing provides individuals with direct access to their genetic information without involving a healthcare provider or insurance company. Individuals can buy the tests online or in stores and submit a DNA sample to the company by mail.[30] Customers receive their results directly from a secure website or in a written report.[31] There are various kinds of DTC-GTs available: ancestry or genealogy, disease risk and health, kinship, and lifestyle.[32]

1. Genetic Ancestry Testing

Genetic ancestry testing or genealogy testing uses DNA variations from SNPs to provide an estimate of ethnic background.[33] Genetic modification is often shared between people from similar backgrounds. [34] Genealogy tests can be used in population genetics to study how people migrated and mixed with other ethnic groups.[35] However, ancestry tests are limited because test results are compared to different databases to identify shared molecular markers.[36]

---

[28] *Id.*
[29] Genetic Testing, *supra* note 22, § DTC Overview; *see generally* Alain Vignal et al., *A Review on SNP and Other Types of Molecular Markers and Their Use in Animal Genetics*, 34 GENETICS SELECTION EVOLUTION 275, 277-78 (2002).
[30] Genetic Testing, *supra* note 22, § DTC Overview.
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] *Id.*

2. Disease Risk and Health

Disease risk and health-based genetic tests estimate an individual's genetic risk of developing common diseases/disorders.[37] These tests may also identify if an individual is a gene carrier for a specific genetic variation/mutation.[38] A genetic carrier inherits a recessive[39] allele for the genetic trait/mutation but does not display the symptoms of the disease or trait.[40] Carriers can pass the recessive allele on to their offspring, and if the offspring acquires another recessive allele from the other parent, the offspring will express the genetic trait/mutation and its symptoms.[41]

Lifestyle tests are a form of disease risk and health-based tests as they inform the consumer how DNA variations may impact lifestyle factors, e.g., fitness, weight loss, nutrition, and sleep.[42] Results are based on an analysis of genetic mutations "that are known or suspected to be associated with the disease or trait."[43]

C. Direct-to-Consumer Genetic Testing Companies

Direct-to-consumer genetic testing companies ("DTC-GTC's") gained prominence with the sequencing of the human genome. These companies provide genome sequencing services directly to the consumer. DTC genetic testing currently has very little regulation or oversight.[44]

---

[37] *Id*.
[38] *Id*.
[39] "Variant masked by the presence of dominant traits but reappears in subsequent generations." *See* Genetic Analysis, *supra* note 2, at 23.
[40] *Id*. at 31-2.
[41] *Id*.
[42] *Id*.
[43] Genetic Testing, *supra* note 22, § DTC Overview.
[44] James W. Hazel et al., *Who Knows What, and When?: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies*, 28 CORNELL J. OF LAW AND PUB. POL'Y 35, 48-50 (2018).

1. Overview of Companies' Policies

The majority of genetic testing companies have privacy policies or terms of services accessible on their websites.[45] However, some of these policies only apply to the use of the company's website and not the specific test kit and genetic information.[46] Some companies only provide additional consent requirements for participation in third-party research.[47] Out of thirty companies' marketing test kits, most companies failed to "consistently meet international transparency guidelines related to confidentiality, privacy, and secondary use of data."[48]

2. Companies' use of Genetic Data

Genetic testing companies sometimes share information with pharmaceutical companies. For instance, 23andMe sells customers' genetic data to GlaxoSmithKline to translate genetic and phenotypic data into targeted pharmaceutical treatments for Parkinson's disease.[49] Other companies share customer data only on an opt-in basis.[50] More than 75 percent of customers agree to participate in the sharing of their data for research in determining disease risk.[51] Although most testing companies only share de-identified data after receiving explicit consent from the consumer, some websites allow people to upload genetic information and search for relatives.[52]

---

[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] Linnea I. Laestadius et al., *All Your Data (Effectively) Belong to Us: Data Practices Among Direct-to-Consumer Genetic Testing Firms*, 19 GENETICS IN MED. 513, 513 (2017).
[49] Press Release, GlaxoSmithKline, GSK and 23andMe Sign Agreement to Leverage Genetic Insights for the Development of Novel Medicines (July 25, 2018) https://www.gsk.com/en-gb/media/press-releases/gsk-and-23andme-sign-agreement-to-leverage-genetic-insights-for-the-development-of-novel-medicines/. [hereinafter GSK].
[50] Julian Segert, UNDERSTANDING OWNERSHIP AND PRIVACY OF GENETIC DATA, Harvard University The Graduate School of Arts and Sciences (2018) http://sitn.hms.harvard.edu/flash/2018/understanding-ownership-privacy-genetic-data/.
[51] *Id.*
[52] *Id.*

GEDMatch's public upload websites helped law enforcement solve the Golden State Killer cold case.[53] Following the Golden State Killer identification, GEDMatch updated its privacy policy to state that genetic data from GEDMatch could be freely used by law enforcement.[54]

Conversely, 23andMe and Ancestry require court orders or valid search warrants before giving third parties or law enforcement access to genetic data records.[55] However, these policies do not guarantee relatives of the individual any protection from future lawful use. As mentioned above in ancestry testing, family members share portions of their genome. So even though the relative does not upload or consent for their genetic information to be shared and utilized, their heritage can still be identified as well as the possibility of identifying disease risk. With the nature of the human genome being individually unique, de-identified information may still allow people to connect the data back to the original person.[56]

III. Genetic Testing Privacy Frameworks

Genetic privacy may be compromised if testing companies remain unregulated and use genetic information in an unauthorized way. Federal and State governments' privacy laws

[53] Linnea M Baudhuin et al, *Privacy In Direct-To-Consumer Genetic Testing*, 65 CLINICAL CHEMISTRY 612, 612-17 (2019) (The police were unable to detect a match through CODIS, so they turned to GEDMatch, a database of genetic information from approximately 900,000 users who have voluntarily uploaded their genetic data after being tested by DTC-GTCs. Through GEDMatch, police were able to trace the serial killer to his great-great-great grandparents and then months later were able to find a branch of the family tree that hailed from the western United States.)

[54] *Id.*

[55] *Id.*

[56] *Id.* DTC genetic testing consumers need to realize that publicly sharing their data allows anyone access to their genetic data, and, by default, they place their family members at privacy risk as well. Consumers assume they will be anonymous; however, researchers have proven that they can rapidly re-identify DTC genetic consumers based on their genetic test results. Consumer re-identification can reveal very sensitive medical information about the donor and even about that person's relatives (particularly if, for example, information about mitochondrial DNA or the Y chromosome is included). It may also be used to connect the donor or a relative to another known DTC genetic consumer; *see also* Yaniv Erlich et al., *Identity Inference Of Genomic Data Using Long-Range Familial Searches*, 362 SCIENCE 690, 690-94 (2018); *see also* Muhammad Naveed et al. *Privacy in the Genomic Era*, 48 ACM COMPUT. SURV. 48 (2015); *see also* Erika Check Hayden, *The Genome Hacker*, 497 NATURE 173 (2013); see *generally* Zhen Lin et al., *Genetics, Genomic Research & Human Subject Privacy*, 305 SCIENCE 183, 183 (2004).

designed to protect consumers' right to privacy vary in terms of their breadth and do not extend to DTC-GTs.[57] Likewise, genetic testing companies' privacy policies range in their comprehensiveness of the public's privacy concerns.[58]

A. Federal Privacy Laws

1. The Fourth Amendment - Searches of DNA Databases by the Government

The Fourth Amendment protects an individual's privacy interest from unreasonable searches and seizures:

> "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, to be supported by Oath or Affirmation and particularly describing the place to be searched, and the persons or things to be seized."[59]

In *Maryland v. King*, the Supreme Court found acceptable genetic searches for individuals with diminished expectations of privacy.[60] A lawful arrest based on probable cause for a "serious" crime permits the police to collect a DNA sample via a cheek swab for identification purposes because it is minimally intrusive.[61] Conducting a DNA test as part of an arrest procedure does not violate the Fourth Amendment's protections because it serves legitimate state interests.[62]

The Fourth Amendment's protections against searches and seizures generally do not apply to genetic information that is voluntarily shared, e.g., with a third party through DTC-GTs. In *United States v. Miller,* the Supreme Court ruled that voluntary data sharing negates expectations

[57] JOHN HOPKINS UNIV., GENETICS & PUB. POL'Y CTR, SURVEY OF DIRECT-TO-CONSUMER TESTING STATUTES AND REGULATIONS (2007) [hereinafter Survey of DTC Statutes and Regulations]; *See, e.g*., Kayte Spector-Bagdady & Elizabeth R. Pike, *Consuming Genomics: Regulating Direct-to-Consumer Genetic and Genomic Information*, 92 NEB. L. REV. 677, 697 (2014).
[58] *Id.*
[59] U.S. CONST. Amend IV.
[60] *Maryland v. King*, 133 S. Ct. 1958 (2013).
[61] *Id.*
[62] *Id.*

of privacy.[63] This rule denies Fourth Amendment protections under the circumstances described above in which DTC genetic test results are openly shared through public upload websites. In these instances, the government does not need to secure a warrant before searching the site for relevant genetic information.

2. Health Information Portability and Accountability Act ("HIPAA")

The HIPAA privacy rule only applies to protected health information of covered entities and their business associates.[64] The privacy rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form of media, whether electronic, paper, or oral.[65] The privacy rule calls this information "protected health information" or "PHI." HIPAA applies to HIPAA covered entities, including a health care provider, a health plan or a health care clearinghouse.[66] Under HIPAA, genetic information is considered health information, and covered entities are prohibited from using and disclosing genetic information for underwriting purposes.[67] DTC-GTC's transmit information electronically, but they are not doctors, clinics, psychologists, dentists, chiropractors, nursing homes, nor pharmacies. DTC-GTs are not covered under HIPAA. Even though genetic tests contain individually identifiable health information this type of information is not protected.

Under HIPAA, a business associate is an entity that performs certain functions or activities on behalf of or provides certain services to, a covered entity that involves the use or disclosure of individually identifiable health information.[68] However, the Act does not consider persons or

[63] *United States v. Miller*, 425 U.S. 435 (1976) (finding defendant had no legitimate expectation of privacy in his bank records because the bank was a third party to which he disclosed his affairs when he opened his account.)
[64] *See* Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 110-233, 122 Stat. 881 (May 21, 2008) Title I, § 105(a); 42 U.S.C.A. § 1320d-9. [hereinafter HIPAA].
[65] *Id.*
[66] *Id*
[67] *Id.*
[68] *Id.*

organizations business associates if their functions or services do not involve the use or disclosure of protected health information.[69] DTC-GTC's are not business associates because they do not perform functions or activities on behalf of a covered entity. However, if the company is providing services on behalf of a physician, the tests are not DTCs but instead physician-ordered genetic tests and subject to HIPAA.

3. Genetic Information Nondiscrimination Act ("GINA")

President Bush signed into law the Genetic Information Nondiscrimination Act on May 21, 2008.[70] Under GINA, genetic information is defined as "any individual, information about (1) such individual's genetic tests, (2) the genetic tests of family members of such individual, and (3) the manifestation of a disease or disorder in family members of such individual."[71] GINA is notable in that it prohibits health insurers from engaging in genetic discrimination and regulates the release of genetic information and employer's requirement of genetic testing.[72] GINA prevents health insurers from increasing premiums or denying coverage to individuals based on genetic information.[73] However, GINA does not apply to life, disability, or long-term care insurance.[74] If DTC-GTC's choose, they can release test results to insurers not covered under GINA upon their request.[75] GINA also does not apply to law enforcement's use of DTC genetic data.[76]

[69] *Id.*
[70] *See* Genetic Information Nondiscrimination Act of 2008, 42 U.S.C. § 2000ff (2008) [hereinafter GINA].
[71] *Id.*
[72] 78 Fed. Reg 5658 (January 25, 2013).
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *Id.*

4. Food and Drug Administration ("FDA")

The FDA classifies DTC-GTs as lower-risk medical devices subjected to the FDA's "regulatory purview."[77] Currently, the FDA regulates a test kit based on how it comes to the market, i.e., a commercial test kit or a laboratory-developed test (LDT).[78] On the one hand, a commercial marketed test kit processes genetic samples packaged together and sold to multiple laboratories.[79] On the other hand, an LDT test kit is developed, performed, and sent to a single laboratory.[80] The FDA chooses not to regulate LDTs for clinical or analytical validity because physicians order the tests.[81]

Generally, the FDA does not review DTC tests for non-medical, low-risk medical, or general wellness purposes.[82] The FDA evaluates moderate and high-risk tests before they can be offered to individuals to assess the tests' analytical and clinical validity.[83] Carrier screening tests that determine whether an individual carries a genetic variant that can be passed down to offspring are exempt from FDA premarket review.[84] Genetic tests intended to provide information about

[77] NAT'L INST. OF HEALTH, NAT'L HUMAN GENOME INST., REGULATION OF GENETIC TESTS (2018) genome.gov/about-genomics/policy-issues/Regulation-of-Genetic-Tests. [hereinafter Regulation of Genetic Tests].
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] FOOD & DRUG ADMIN. DIRECT-TO-CONSUMER TESTS, MEDICAL DEVICES: IN VITRO DIAGNOSTICS https://www.fda.gov/medical-devices/vitro-diagnostics/direct-consumer-tests.
[83] *Id.*; The FDA authorized 23andMe to offer a direct-to-consumer carrier status test for Bloom Syndrome in February 2015, subsequently authorized it to carry out Genetic Health Risk (GHR) tests for ten diseases in April 2017, and mostly recently, authorized a test that reports on three mutations in BRCA genes in March 2018. As part of the pre-market approval process for GHR tests, 23andMe was required to demonstrate the analytical validity of their tests as well as adequate consumer understanding of the sample collection process and the resulting genetic reports. Going forward, the FDA "intends to exempt additional 23andMe GHR tests from the FDA's premarket review, and GHR tests from other makers may be exempt after submitting their first premarket notification . . . allow[ing] other, similar tests to enter the market as quickly as possible and in the least burdensome way, after a one-time FDA review." Press Release, Fed. Drug Admin., FDA Allows Marketing of First Direct-to-Consumer Tests that Provide Genetic Risk Information for Certain Conditions (April 6, 2017), https://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm551185.htm; *See also* Press Release, Fed. Drug. Admin., FDA Permits Marketing of First Direct-to-Consumer Genetic Carrier Test for Bloom Syndrome (Feb. 23, 2015), https://www.fda.gov/newsevents/newsroom/pressannouncements/ucm435003.htm.
[84] 21 CFR 866.5940.

specific medical conditions or diseases, and tests designed to provide information explaining medication side effects and genetic interaction are required to obtain FDA clearance before DTC-GTCs can offer the tests.[85]

5. Clinical Laboratory Improvement Act ("CLIA")

The FDA and the Centers for Medicare and Medicaid Services ("CMS") have the authority to regulate genetic tests.[86] However, CMS regulation only extends to the analytical validity[87] of the tests, not to the protection of individual private information.[88] CMS regulates clinical laboratories through CLIA, which establishes a certification process for laboratories to process medical samples.[89] While CLIA determines clinical testing quality, including verifying the procedures used, it does not examine whether tests are clinically valid or whether safeguards are in place to protect individual privacy.[90]

Laboratories' compliance with CLIA depends on the nature and complexity of the tests performed. CLIA classifies most genetic tests as moderate or high-complexity laboratory tests.[91] Laboratories that only perform tests that are simple laboratory examinations and procedures that pose no reasonable risk of harm if performed incorrectly may qualify for a certificate of waiver.[92] Moderate and high-complexity tests require a certificate of compliance by CMS.[93] Laboratories

[85] 21 CFR 866.5950; 21 CFR 862.3364.
[86] Regulation of Genetic Tests, *supra* note 77.
[87] *Id.* Analytical validity refers to how well the test predicts a genetic change.
[88] *Id.*
[89] *Id.*
[90] *Id.*
[91] NAT'L INST. OF HEALTH, NAT'L HUMAN GENOME INST., THE CLIA FRAMEWORK, (2018) https://www.genome.gov/Pages/PolicyEthics/GeneticTesting/The_CLIA_Framework.pdf. [hereinafter CLIA Framework].
[92] 42 CFR 493.15.
[93] CLIA Framework, *supra* note 91.

that perform genetic tests have the option to either go through a proficiency testing program or evaluate their testing programs at least twice a year.[94]

Clinical laboratories that comply with CLIA may release information "for the diagnosis, prevention, or treatment of any disease or impairment of, or the assessment of the health of, human beings."[95] Laboratories are exempt from CLIA requirements if they are "research laboratories that test human specimens but do not report patient-specific results for the diagnosis, prevention or treatment of any disease or impairment of, or the assessment of the health of individual patients."[96]

Here, DTC-GTCs do not need to comply with CLIA because they communicate test results to consumers, not for the diagnosis, prevention, or treatment of any disease or impairment. DTC-GTCs purpose is for consumers to obtain information related to ancestry, risk of disease, and non-clinical traits (hair color, earlobe type). LDTs, as discussed above, would need to comply with CLIA requirements as they are moderate or high complexity tests.

6. Federal Trade Commission ("FTC") Privacy Protection Laws

The FTC recommends that consumers scrutinize the company's website and privacy practices regarding how genomic data is used, stored, and disclosed before buying a test kit.[97] Although the FTC does not provide genetic privacy protection, it can take action against companies that do not safeguard consumers' personal data.[98] The FTC also has broad authority to police unfair

---

[94] CLIA Framework, *supra* note 91. *See also* 42 CFR 493.801(2)(ii).
[95] 42 U.S.C. 263a.
[96] 42 CFR 493.3(2).
[97] U.S. FED. TRADE COMM'N, DIRECT-TO-CONSUMER GENETIC TESTS, (2018); *See also* U.S. FED. TRADE COMM'N, DNA TEST KITS: CONSIDER THE PRIVACY IMPLICATIONS, (2017).
[98] *See generally LabMD v. FTC*, 1:14-cv-00810-WSD (11th Cir. 2019) (LabMD engaged in unreasonable data security practices that resulted in the unauthorized sharing of sensitive medical information. FTC concluded privacy harm is a substantial injury to consumers and LabMD must establish a comprehensive information security program subject to assessments); *see also* Press Release, U.S. Fed. Trade Comm'n, FTC Announces Settlements with Four Companies Related to Allegations they Deceived Consumers over Participation in the EU-Privacy Shield, (Dec. 3, 2019) https://www.ftc.gov/news-events/press-releases/2019/12/ftc-announces-settlements-four-companies-related-allegations-they.

and deceptive practices under the FTC Act.[99] The only meaningful action the FTC took was against GeneLink in 2014 for health-related claims not supported by the evidence, and data security practices that rose to the level of unfair and deceptive.[100] The Health Breach Notification Rule requires businesses not covered by HIPAA to notify customers if there is a breach of "unsecured, individually identifiable electronic health information."[101] The rule applies to a vendor of personal health records who maintains an online service that allows consumers to share, organize, and manage identifiable health information drawn from multiple sources e.g. maintaining medical records in a physician's mobile application to upload changes in weight, blood pressure, and diet.[102]

DTC-GTCs will be subject to the FTC's oversight regarding compliance with the EU-Privacy Shield and data security practices. However, the health breach notification rule does not apply to DTC-GTCs because they are not a vendor, i.e., they do not maintain a service for patients to access and upload changes to medical records.

7. Common Rule for Clinical Research

The Common Rule mandates that research involving FDA-regulated products or research conducted or supported by a federal agency must seek Institutional Review Board ("IRB") approval before conducting studies involving human subjects.[103] Research projects limited to

[99] Fed. Trade Comm'n Act of 1914 15 U.S.C. §§41-58 (2018).
[100] *In Re GeneLink, Inc. & Foru Int'l Corp.*, No. 112-3095 U.S. Fed. Trade Comm'n (Jan. 7, 2014).
[101] *Health Breach Notification Rule*, U.S. Fed. Trade Comm'n.
[102] *Id.*
[103] Ernest D. Prentice & Bruce G. Gordon, *Institutional Review Board Assessment of Risks and Benefits Associated with Research*, 2 NAT'L BIOETHICS ADVISORY COMM'N, ETHICAL & POL'Y ISSUES IN RESEARCH INVOLVING HUMAN PARTICIPANTS, 1 (2001).

publicly available data are not subject to IRB review.[104] Researchers do not need prior IRB approval for aggregated and de-identified genetic information.[105]

DTC-GTCs have added research opportunities where customers can share their genetic information for use in research (23andWe, and Navigenics).[106] 23andMe's research division, called 23andWe, is structured to investigate the causes of diseases and develops drugs and treatments accordingly.[107] 23andWe incorporates a large pool of samples from consumers participating in standard test kits and establishes location-based clinical trials.[108] Research participants of the clinical trials contribute their genetic information and health background prompted by online surveys.[109] Other DTC-GTCs like Navigenics "believe in … helping further scientific and medical research."[110] The company may use consumers' genetic data to "discover and validate associations between certain genetic variations and certain health conditions or traits."[111] Navigenics findings may be published "without disclosing Genetic Data sufficient to uniquely identify [participants]."[112] deCODEme also invites its customers to participate in research activities.[113] Private-based DTC-GTCs are not required to seek IRB approval for research projects as they do not receive federal funding and are not subject to federal regulations.

---

[104] 45 CFR 46.102(b)(4).
[105] 45 CFR 46.102(f) biological specimens or private information is identifiable when it can be linked directly or indirectly to a specific individual, when this information is obtained for research purposes it constitutes as human subjects research. *See also* U.S. DEPT. OF HEALTH AND HUMAN SERVICES, OFFICE FOR HUMAN RESEARCH PROTECTIONS, GUIDANCE ON CODED PRIVATE INFORMATION OR SPECIMENS USE IN RESEARCH, (2008) https://www.hhs.gov/ohrp/regulations-and-policy/guidance/research-involving-coded-private-information/index.html.
[106] 45 CFR 46.102(b)(4).
[107] Consent Document, 23andMe, https://www.23andme.com/about/consent.
[108] Research Revolution, 23andMe, https://www.23andme.com/researchrevolution.
[109] Consent Document, *supra* note 107.
[110] Privacy Policy, Navigenics, http://www.navigenics.com/visitor/what_we_offer/our_policies/privacy.
[111] *Id*.
[112] *Id*.
[113] Terms of Use, deCODEme, http://decodeme.com/terms-of-use.

B. State Privacy Laws

Most states have enacted legislation to prohibit insurers from collecting or using genetic information to discriminate.[114]

1. California Consumer Privacy Act ("CCPA")

The CCPA provides California residents with the right to (1) know what personal data[115] is collected about them; (2) be notified of sale or disclosure of personal data; (3) object to the sale of personal data; (4) access their data; (5) freedom to exercise their rights without fear of discrimination; and (6) request a business to delete any acquired personal data.[116] CCPA applies to any organization that does business in California and has either (1) annual gross revenues greater than $25 million; (2) earns more than half of its revenue from selling consumers' personal information or (3) maintains the personal information of 50,000 or more consumers.[117] Corporations are required to (1) designate methods for submitting data access requests;[118] (2) update privacy policies to include a description of residents' rights;[119] and (3) the company's website must have an opt-out link on the homepage to "Do Not Sell My Personal Information."[120] Companies who do not comply may be fined up to $7,500 for each intentional violation, $2,500

[114] NAT'L CONFERENCE OF STATE LEGISLATORS, STATE GENETIC PRIVACY LAWS, http://www.ncsl.org/research/health/genetic-nondiscrimination-in-healht-insurance-laws.aspx [hereinafter State Privacy Laws].
[115] Cal. Civ. Code §1798.140; Cal. Civ. Code §1798.185(k)(2). Personal data is information that "relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household such as a real name, alias, postal address, unique personal identifier, IP address, email address, account name, SSN #, or other similar identifiers. Personal data includes biometric information which means an individual's physiological, biological or behavioral characteristics, including an individual's DNA, that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Publicly available does not mean biometric data collected by a business about a consumer without the consumer's knowledge. Publicly available also does not include consumer information that is de-identified or aggregated.
[116] Title 1.81.5 The California Consumer Privacy Act of 2018 § 1798.110.
[117] *Id.*
[118] Cal. Civ. Code §1798.130(a).
[119] Cal. Civ. Code §1798.135(a)(2).
[120] Cal. Civ. Code §1798.102.

for each unintentional violation, and statutory damages between $100-$750 per California resident if they become victims of data theft or breach.[121]

23andMe is subjected to CCPA because it maintains personal information, including biometric data of more than 50,000 consumers, has annual gross revenue over $25 million, and conducts business in California.[122] Because not every aspect of 23andMe's business takes place outside of California, CCPA restricts the business' ability to collect or sell consumers' personal information. Anything de-identified or aggregated under CCPA is not considered publicly available and is subject to the Act's compliance.

2. Other State Laws and Regulations

States' privacy protections vary.[123] Some states mandate individual access to personal genetic information.[124] Genetic information is defined as "personal property" in Alaska, Colorado, Florida, Georgia, and Louisiana.[125] Likewise, Rhode Island and Washington require companies to receive written authorization to disclose genetic information.[126] Forty-seven states prohibit the use of genetic information to determine rates of insurance eligibility.[127] Twenty-seven states require informed consent for a third party to perform or request a genetic test or to obtain genetic information.[128] Eighteen states have specific penalties for violating genetic privacy laws.[129] One state extends personal property rights to DNA samples.[130]

---

[121] Cal. Civ. Code §1798.150, 155.
[122] 23andMe 10K ($475 million annual gross revenue and headquarters is located in Mountainview, California).
[123] State Privacy Laws, *supra* note 114.
[124] *Id*.
[125] *Id*.
[126] *Id*.
[127] *Id*.
[128] *Id*.
[129] *Id*.
[130] *Id*.

C. International Transparency Standards – General Data Protection Regulation

In May 2018, the European Union ("EU") launched the General Data Protection Regulation ("GDPR") to protect the "fundamental rights and freedoms of natural persons and their right to the protection of personal data."[131] GDPR applies to all companies, not just healthcare providers or insurance companies. GDPR defines personal health data to include:

> "all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration form, or the provision of, health care services as…a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, ***including from Genetic Data and biological samples***; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test."[132]

GDPR is legally binding for United States businesses with global operations, international sites, or even remote workers.[133] The GDPR defines genetic data as personal data

> "relating to the inherited or acquired genetic characteristics of a natural person which result from the analysis of a biological sample from the natural person in question, in particular chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or from the analysis of another element enabling equivalent information to be obtained."[134]

Any test results acquired from DTC-GTs create genetic data, and as such, any testing companies that function in the EU must adhere to GDPR for personal data and consent. Under GDPR,

---

[131] Art. 1 GDPR Subject-matter and objectives.
[132] Recital 35 EU General Data Protection Regulation [emphasis added].
[133] Art. 3 GDPR Territorial Scope. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, ***regardless of whether the processing takes place in the Union or not***. This Regulation applies to ***the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (1) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (2) the monitoring of their behavior as far as their behavior takes place within the Union***. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law. [emphasis added].
[134] Recital 34 *Genetic Data*, General Data Protection Regulation.

processing of personal data requires approval from the data subject or an expressed provision of law.[135] GDPR also requires the right of EU citizens to be informed about the storage and use of their data.[136] A company must immediately notify individuals when obtaining their data.[137]

Companies like 23andMe and Ancestry that are global companies offering consumer health services would be considered controllers under the GDPR. As a controller, these testing companies are responsible for maintaining the protection of personal data through consent and processing requirements.

D. Future of Privacy Forum Best Practices

The Future of Privacy Forum established voluntary privacy best practices for consumer genetic testing services.[138] Companies' privacy practices are required to maintain complete transparency about how genetic data is collected, used, shared, and retained.[139] The privacy disclosure must include publicly posting a high-level summary of privacy protections easily accessible to consumers.[140] Companies must have a separate express consent for the transfer of genetic information to third parties and are banned from sharing the information with employers,

---

[135] Recital 32 *Conditions for Consent*, General Data Protection Regulation; *See also* Art 7. GDPR Conditions for Consent: (1) freely given on a voluntary basis; (2) must notify fata subject of controller's identity, what of data will be processed, how it will be used and the purpose of the processing operation; (3) must inform data subject of their right to withdraw consent at any time; and (4) consent requires a clear statement or affirmative act.

[136] Art. 12 GDPR Transparent information, communication and modalities for the exercise of the rights of the data subject; Art. 13 GDPR Information to be provided where personal data are collected from the data subject; Art. 14 GDPR Information to be provided where personal data have not been obtained from the data subject. [hereinafter Information Transparency].

[137] Information Transparency, *supra* note 136. The controller's obligation to inform includes his identity, the contact data of the Data Protection Officer (if available), the processing purposes and the legal basis, any legitimate interests pursued, the recipients when transmitting personal data, and any intention to transfer personal data to third countries. The right to be informed also includes information about the duration of storage, the rights of the data subject, the ability to withdraw consent, the right to lodge a complaint with the authorities and whether the provision of personal data is a statutory or contractual requirement.

[138] FUTURE OF PRIVACY FORUM, PRIVACY BEST PRACTICES FOR CONSUMER GENETIC TESTING SERVICES, (July 31, 2018) https://www.healthlawadvisor.com/files/2019/06/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf. [hereinafter Future of Privacy Forum].

[139] *Id.*

[140] *Id.*

insurance companies, educational institutions, and government agencies without consent unless required by law.[141] However, DTC-GTCs are not required to participate in the future of privacy forum, and only a select number of companies are supporters of the best practices, including 23andMe, Ancestry, MyHeritage, Helix, Habit, African Ancestry, and Living DNA.[142] If a company's policy conflicts with the best practices, the forum will remove the company as a supporter.[143]

E. Genetic Testing Companies' Privacy Policies

Both 23andMe and Ancestry present customers with two documents upon purchasing a test kit. The first document the companies present are the terms and conditions that include a privacy statement. The second document is an informed consent document. Customers must accept the terms and conditions before they can buy a test kit from the company. The informed consent document is presented to consumers when they are registering their test kit as it relates to additional research projects run by the company, e.g., 23andWe. Both 23andMe and Ancestry have a history of sharing anonymized consumer data with third parties.

1. 23andMe

23andMe's website contains very detailed privacy statements, which address how the company collects, manipulates, and protects genetic information.[144] The website defines personal information as "information that can be used to identify a user either alone or in combination with other information."[145] Personal information is broken down into genetic information (data

[141] *Id.*
[142] *Id.*
[143] *Id.* FamilyTreeDNA was removed as a supported following their agreement with the FBI.
[144] Privacy Statement, 23andMe, https://www.23andme.com/about/privacy/; Terms of Service, 23andMe, https://www.23andme.com/about/tos.
[145] *Id.*

generated by processing a user's DNA sample), registration information (name, email address, etc. used to create an account or purchase test kits), and self-reported information (user's response to surveys).[146]

23andMe requires users to complete two informed consent documents.[147] The main research consent document includes that 23andMe can use individual-level genetic information and self-reported information internally.[148] For third party research purposes, the information must be de-identified and not linked to registration information.[149] The company also provides an individual-level data sharing consent form which includes the same uses as above and that 23andMe may share de-identified individual-level genetic information and self-reported information with select third party research contributors.[150] The document also allows users to withdraw consent by changing their consent status in their account settings.[151] However, once data is shared with third parties, it will not be withdrawn.[152] 23andMe also does not state how it protects the confidentiality of the shared information or how it prohibits attempts to re-identify individuals. 23andMe is also committed to compliance with GDPR.[153]

23andMe maintains different levels of data sharing.[154] Users' aggregate data, individual-level genetic information, and self-reported information may be shared as specified in the consent document.[155] 23andMe may share with both commercial third parties, and non-profits

[146] *Id*.
[147] Research Consent Document, 23andMe, https://www.23andme.com/about/consent/; Terms of Service, *supra* note 144.
[148] *Id*.
[149] Research Consent Document, *supra* note 147.
[150] *Id*.
[151] *Id*.
[152] *Id*.
[153] Data Protection, 23andMe, https://www.23andme.com/gdpr/?vip=true
[154] *Id*.
[155] *Id*.

aggregated[156] genetic and self-reported data.[157] De-identified genetic information may be published in peer-review journals and other research funded by the federal government (NIH) conducted by 23andMe.[158] 23andMe research may be sponsored, conducted on behalf, or in collaboration with third parties (foundations, academic institutions and pharmaceutical companies).[159]

2. Ancestry DNA

Ancestry DNA states customers' genetic data will be used correctly for: "genetic and genealogical research, including population health and ethnicity-related analyses, and not to provide you individual medical or diagnostic purposes."[160] Put another way, Ancestry uses genetic information to provide customers with ancestry results and identify relatives based on similar DNA molecular markers. The company also states that consumer data is de-identified to make discoveries in population genetics.[161] Ancestry DNA's privacy policy contains three significant provisions: "(1) the perpetual, royalty-free, worldwide license to use your DNA; (2) the warning that DNA information may be used against 'you or a genetic relative'; and (3) your waiver of legal rights."[162] These provisions give a written warning to Ancestry customers but are embedded in "click-wrap" (requiring the user to "agree" upon ordering the kit, which most consumers consent

[156] Privacy Statement, *supra* note 144. "It has been stripped of registration information and combined with data from other users to minimize the possibility of exposing individual-level information." Aggregate data is information combined with other users and analyzed or evaluated as a whole with no specific individual identified. e.g., 30% of our female users share a particular genetic trait. Individual information is information about a single individual's genotypes, diseases or other traits/characteristics.
[157] *Id*.
[158] *Id*. "If you choose to consent to participate in 23andMe Research, 23andMe researchers can include your de-identified genetic information and self-reported information in a large pool of customer data for analyses aimed at making scientific discoveries."
[159] *Id*.
[160] Privacy Statement, Ancestry, https://www.ancestry.com/cs/legal/privacystatement
[161] *Id*.
[162] *Id*.

to without reading the entire agreement) or "browser-wrap" (implies consent by use of the website) agreements.[163] Furthermore, Ancestry maintains ownership of the customers' DNA in perpetuity.[164]

3. Personal Genome Project

Harvard School of Medicine's Personal Genome Project ("PGP") publishes all information submitted by a participant, including physical traits, medical information, and photographs on PGP's public website along with genetic information.[165] While individuals interested in participating must submit to a rigorous pre-enrollment questionnaire and consent process, family members do not.[166] Once PGP releases the information, neither PGP nor the participant can control who has access, can make copies, or use the information.[167] This poses a concern for the individual as well as family members because "anyone with sufficient knowledge and resources" could use the data to claim a participant is predisposed to a disease, or they are related to criminals.[168]

4. Burying Privacy Disclaimers in Terms and Conditions

While genetic testing companies claim to have privacy protections surrounding genetic information, most of the policies follow a take it or leave it approach. If individuals do not consent to the privacy statements, they cannot obtain a DTC-GT. Consumers consent to collecting risk information and disclosure of results by clicking "yes" on a dialogue box. The mere click should not be considered informed consent unless consumers spend the time to read the disclosure in its

---

[163] Andelka M. Phillips, *Reading the Fine Print When Buying Your Genetic Self Online: Direct-to-Consumer Genetic Testing Terms and Conditions*, 36 NEW GENETICS & SOC'Y 278 (2017).
[164] *Id*.
[165] Personal Genome Project, Consent Form: Personal Genome Project § X:10.1 (2010), http://www.personalgenomes.org/consent/PGP_Consent_Approved03312010.pdf [hereinafter Full Consent].
[166] Personal Genome Project, Consent Form: Eligibility Screening for the Personal Genome Project § 1 (2010), available at http://www.personalgenomes.org/consent/PGP_MiniConsent_Approved03312010.pdf [hereinafter Mini Consent]; How It Works, Personal Genome Project. http://www.personalgenomes.org/howitworks.html.
[167] *Id*.
[168] Full Consent, *supra* note 165, at § VII:7.1(a)(iii).

entirety.[169] Consenting to terms and conditions by clicking on an "accept" or "yes" dialogue box is now very commonplace given the bombardment of consumers downloading applications and routine operating system updates, which most people consent to without reading the statements.[170] If customers of DTC-GTs operate reading the permission in the same way that they consent to system updates, they are genuinely not informed. Companies can bury privacy information, the length samples will be kept, and means of selling genetic information in the "informed consent" without customers knowing how their genetic information is being stored and manipulated. The gaps in privacy regulations cause consumers to agree to security protections absentmindedly and as routine as clicking through website terms and conditions.

IV. Gaps in Existing Consumer Protection

Despite the existing federal and state safeguards, some of these laws still do not adequately address privacy issues and consumer protection related to genomic data. Consumers may believe that HIPAA protects their information yet, HIPAA does not cover DTC genetic testing companies as detailed above. Both CLIA and the FDA continue to have a regulatory gap with no oversight to protect individual privacy when analyzing DTC-GTs. The FTC has done very little to enforce companies' privacy compliance. Nevertheless, privacy concerns persist with the sharing of de-

[169] Joel R. Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 485 (2014).

[170] *Tompkins v. 23andMe, Inc.*, 840 F.3d 1016, 1020 (9th Cir. 2016) (A customer interested in obtaining the genetic test must visit the 23andMe website to purchase an online DNA testing kit. When purchasing the kit, the customer can click on a link to the company's Terms of Service that was available at the bottom of the webpage. However, the customer is not required to read or click through the terms before making a purchase. After receiving the kit, the customer returns to the website to create an online account with 23andMe to register the DNA kit. At this stage, and in order to proceed to use the genetic testing service, a customer has to click on a box indicating agreement to the Terms of Service. The Terms of Service is a multipage agreement which states that it constitutes the entire agreement between 23andMe and its customers.)

identified information because, with emerging technology, third parties may misuse this information and is not truly de-identified.[171]

A. Potential for Third-Party Misuse of Data

Whole exome and whole-genome sequencing, as mentioned above, rely on sharing data by looking at the genomic sequences of large populations of people. However, there are concerns that this technology will affect individual privacy with the increased number of individuals who can access the data leading to misuse or breach. The misuse or breach of data stems from recent events involving electronic health record breaches.[172]

Several state statutes require the preservation of DNA samples.[173] Preservation of the sample allows future testing of the sample when new technologies become available.[174] The preservation of the sample also raises concerns about physicians' misuse of consumer health information.[175] However, physicians are HIPAA covered entities and cannot share PHI for marketing tactics unless they fall into a HIPAA exception.[176]

Conversely, DTC-GTCs may misuse consumer health information for marketing since there are no regulatory requirements in place to govern the use of personal data. While physicians cannot manipulate genetic information, DTC-GTCs are not HIPAA covered entities, and no other federal or state laws prohibit testing companies' use of genetic information for promotional

[171] Future Privacy Forum, *supra*, note 138.
[172] W.W. Koczkodaj, et al., *Electronic Health Record Breaches as Social Indicators,* 141 SOC. INDIC. RES. 861, 861–871 (2019).
[173] *See* ALA Code § 36-18-22 (Supp. 1994); CAL Penal Code § 290.2 ; N.C Gen Stat. §15A-266.5(b); VA Code Ann. § 19.2-310.3.
[174] *Id.*
[175] C. Critchley et al., *Public reaction to direct-to-consumer online genetic tests: Comparing attitudes, trust and intentions across commercial and conventional providers*, 24 PUBLIC UNDERST. SCI. 731, 731–750 (2014).
[176] HIPAA, *supra*, note 64.

purposes. Testing companies governed by GDPR cannot process, store, or share genetic information with third parties without the express permission of the individual.

There is also the potential for misuse of data in what is being called "DNA theft."[177] There is an increased risk that "third parties may attempt to collect and analyze anyone's DNA without consent."[178] Since DTC-GTCs only require a customer to accept the company's terms and conditions before purchasing a kit, individuals may submit another person's sample without their knowledge or consent. Public databases like PGP and GEDMatch could also result in false claims of a criminal relationship or disease predisposition if someone altered and republished the same data obtained from DTC-GTCs. Someone could also make synthetic DNA from the public database and plant it at a crime scene to implicate a person in a crime.

B. Using Molecular Markers to De-Anonymize Genetic Data

The nature of genetics is information taken from one person's genetic composition that may be shared with biological siblings and offspring.[179] For this reason, genetic information is considered sensitive, primarily since it can also determine predisposition to a gene that could affect an individual or a family.[180] Genetic data can be de-anonymized by genetic markers tied to specific physical traits like hair and eye color.[181] The physical characteristics can be cross-referenced with publicly available data to identify whom the DNA belongs to.[182]

---

[177] Elizabeth E. Joh, *DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing*, 91 B.U. L. Rev. 665 (2011); *see also* Eriq Gardner, *Gene Swipe: Few DNA Labs Know Whether Chromosomes Are Yours or If You Stole Them*, 97-AUG A.B.A. J. 50 (2011).
[178] *Id*.
[179] Genetic Analysis, *supra*, note 2, at 4.
[180] *Id*.
[181] *Id*. at 6-7.
[182] Genetic Testing, *supra*, note 22.

People believe a "robust anonymization assumption" that by removing specific identifiers, the individual would remain anonymous.[183] The NIH removed some genetic data from publicly available websites[184] following a study that identified a single individual's DNA contribution from a pool of a thousand samples.[185] Another example deals with the Massachusetts Group Insurance Commission's removal of explicit identifiers where researchers were able to de-identify patient records and identify the governor.[186] As previously discussed, SNPs are useful in DTC-GTs because they correspond to both non-clinical and clinical traits. A study in 2004 determined that thirty SNPs can be used to identify a single person out of the millions of SNPs analyzed in a genetic test.[187] Someone who has access to both anonymized genetic data and public data may be able to de-anonymize the data and identify an individual with a small set of SNPs. Scientists can also determine a person's surname by studying the short tandem repeats on the Y chromosome and linking that with publicly available information.[188]

Any form of genetic information sharing through the public domain or for research (DTC-GTCs information sharing with third-parties and non-profit research institutions) creates the possibility that someone will access the data and re-identify the set. As mentioned in PGP's overview, this poses a concern for the individual as well as family members. The gaps in protection implicate autonomy and privacy for family members who do not want to share their genetic information or know risk facts that their relatives' DNA might reveal.

---

[183] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1706 (2010). [hereinafter Broken Promises of Privacy].
[184] Jennifer Couzin, *Whole-Genome Data Not Anonymous, Challenging Assumptions*, 321 SCIENCE 1278, 1278 (2008).
[185] Nils Homer et al., *Resolving Individuals Contributing Trace Amounts of DNA to Highly Complex Mixtures Using High-Density SNP Genotyping Microarrays*, 4 PLoS Genetics 1, 7 (2008). .
[186] Broken Promises of Privacy, *supra* note 183, at 1719-20.
[187] Zhen Lin et al., *Genetics, Genomic Research & Human Subject Privacy*, 305 SCIENCE 183, 183 (2004).
[188] Melissa Gymrek et al., *Identifying Personal Genomes by Surname Inference*, 339 SCIENCE 321, 321-24 (2013).

C. Access to Genetic Information by Life, Disability, and Long-Term Care Insurance

The dangers of misinterpretation of genetic information attribute to the fears of gene testing, genetic discrimination, and insurance coverage. For instance, genetic tests could previously lead to discrimination by insurance companies in terms of health care coverage.[189] Though under GINA genetic discrimination is prohibited by corporations and health insurers, genetic tests also bring about concerns for life, disability, and long-term care insurance coverage.[190]

Genetic test results have led to manipulation by life, disability, and long-term care insurance companies. Companies that offer these policies have the right to request genetic test results when making decisions about coverage and insurance premiums.[191] Insurance companies then use this information to place people into groups based on risks. Specifically, if a genetic test was shown as part of the patient's medical history, insurance companies could use this information to determine coverage for life and disability insurance.

Nevertheless, just because someone has a predisposition to something, there is no guarantee they will manifest the disease during their insurance period. If the individual did not disclose the test results, they would be evaluated as less risky and have slightly better premiums. Additionally, physicians include genetic results from tests they order into the patient's medical record, and the insurance company will most likely have access to that information. Given the consent forms DTC-GTCs require consumers to submit for research purposes, DTC-GT results hopefully are secure from the insurance companies' access. Due to genetic discrimination in these

[189] "Fears of genetic discrimination by employers and insurance companies continue to influence decisions regarding submission to genetic testing and participation in certain forms of genetic research." PHYLLIS GRIFFIN EPPS, GENETIC DISCRIMINATION, 2 ENCYC. OF BIOETHICS, (3rd ed. 2004).
[190] *Id*.
[191] Genetic Testing, *supra* note 22, § Can Results Affect Insurance?

types of insurance, people may avoid genetic tests for fear that taking the test or getting a positive result could affect their coverage.

V. Consideration of Mechanisms to Maintain Individual Privacy

The United States needs new genetic privacy laws to protect individual privacy, related explicitly to DTC-GTs. Providing privacy protections should be maintained on a federal level, not on a state-by-state basis. State-based privacy protections would not solve consumers' privacy concerns, as some states may allow sharing of genetic information that could link a family member who does not want their information shared from a state with more stringent privacy protections. The federal government should focus on either applying a standard like GDPR or modify what is classified as a HIPAA covered entity. The main difference between the structure of GDPR and HIPAA is that GDPR defines entities based on ownership of data, and HIPAA defines entities based on the function of the organization.

A. Expansion of HIPAA and GINA

Congress should amend HIPAA to include genetic testing companies as covered entities under HIPAA. Most consumers assume their genetic information is stored and protected following HIPAA regulations. However, as discussed above, that is not the case. HIPAA does not govern the activities of genetic testing companies because they are not considered covered entities or business associates. Consumers must then agree to privacy and security protections through click-through policies. If genetic testing companies were classified as covered entities, because they already transmit information in an electronic form, they could not share consumers' genetic information. A criticism to this approach, is that by preventing information sharing it halts scientific growth and expansion. Anonymized consumer genetic information may be helpful in identifying diseases or genetic irregularities in various communities through population genetics

as researchers can have access to large sample sizes. However, the drawbacks to expanding HIPAA do not outweigh protecting consumer privacy interests, as individuals can still elect to have DTC-GTCs sell their data.

Congress should also expand GINA to include protection of all genetic data regardless of the source of that information. In conjunction with the HIPAA expansion, this would help to ameliorate some of the effects of data misuse and insurance discrimination while boosting consumer participation in buying test kits. The FDA and CLIA could also regulate DTC-GTC's commercial test kits in the same manner that they regulate LDTs ordered by physicians. The proposed changes would fill in some gaps, but it would not prevent re-identification from public domain uploads.

B. Protection Against Re-identification and Restricting Research

A primary unintended consequence of data sharing, DTC-GTs, and genetic research is the misuse of data and de-anonymization. Congress could expand the Common Rule to include all research projects, whether implemented by private companies or those under federal grants/regulations. Then DTC-GTCs would have to draft research proposals and consent documents for IRB approval before sharing genetic information with third parties and pharmaceutical companies. However, DTC-GTCs are unlikely to support this change because it may prevent research opportunities and minimize the profit DTC-GTCs can receive for selling genetic data to pharmaceutical companies.

Another solution is to have consumers maintain ownership of their data. In turn, genetic testing companies would provide customers with a complete readout of their genome that the individual could anonymously share with whomever at their choosing, including third-party pharmaceutical companies interested in marketing drugs to individuals based on genetic markers.

This structure is like GDPR right to data portability in which subjects have the right to receive and transmit their data with whom they see fit without any hindrance.[192] However, this may also lead to re-identification if the information ends up in the wrong hands. Furthermore, data portability requirements would be inapplicable to PGP's structure because one of its goals is unrestricted, public sharing.

C. GDPR-like Regulatory Framework

The best approach is to apply a federal privacy standard similar to how the EU structured the GDPR by requiring notification of when personal data is obtained and how the records are processed. GDPR processing requirements would still allow the federal government to access personal data relating to criminal convictions or offenses.[193] The GDPR fines[194] also provide companies incentives to maintain compliance with the regulations. Researchers that share biological samples that contain genetic information would be held to personal data protection standards. This approach would require researchers to notify individuals when biological samples are processed and obtain express consent from the individuals before processing information and sharing it with third parties. The GDPR also requires data to be destroyed once the relationship between the controller and the processor ends. By implying this requirement, it limits the ability to aggregate and retain personal data for future use, which in turn can prevent the potential for third-party misuse of data and reduce/eliminate de-anonymizing genetic data. While this may not

[192] Art. 20 GDPR Right to Data Portability.

[193] Art. 10 GDPR Processing of personal data relating to criminal convictions and offences. Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.

[194] If a company does not maintain records of processing activities and/or does not provide a complete index to authorities, they are subject to fines according to Art. 83(4)(a) of the GDPR. The possible fines can be up to 10 million euros or 4% of their annual turnover. This total is, as a rule, only assessed by the authorities in exceptional cases. For this, the authorities are encouraged, as set forth in recital 13, "to take account of the specific needs of micro, small and medium-sized enterprises in the application of this Regulation."

be a perfect solution, it gives consumers more control over their personal information even though it may dissuade companies from selling or utilizing consumers' data.

VI. Conclusion

DTC-GTC's need to implement robust privacy and security programs to mitigate the gaps in regulation with improved data storing and sharing security. Currently, there are no precise regulatory mechanisms in place to protect patient autonomy and individual privacy. Because so much can be gained from DTC-GTs and genetic research, participation should be protected where possible. At a minimum, Congress should expand HIPAA and GINA to cover all genetic information no matter where the data is obtained. Nevertheless, the best approach is to enact a GDPR-like regulatory framework that would promote individual autonomy and privacy while fostering a collaborative research environment.