PROTECTING CONSUMERS AND REGULATING DATA: THE NEED FOR COMPREHENSIVE FEDERAL OVERSIGHT OF THE DIRECT-TO-CONSUMER GENETIC TESTING INDUSTRY

*Kevin C. Gilligan**

ABSTRACT

The Direct-to-Consumer (DTC) genetic testing market is a massive biotechnology industry. Millions of people take at-home genetic tests for many reasons, ranging from pure curiosity to learning about a person's genetic predispositions for diseases. This industry is one of many great accomplishments of modern science because it sequences a person's genome and provides useful results to that person. The cornerstone of the DTC genetic testing industry is data collection. But this is not normal data collection. This is data collection of peoples' genomes. Genetic information is immutable information, and as such, it must be safeguarded. However, current laws largely do not regulate this industry in regard to securing and sharing genetic data. And self-regulation of an industry dealing with precious data could prove harmful to people who use this industry.

Databases get breached, and information gets stolen. But instead of having one's credit card number stolen, a person whose data is stolen from a genetic testing database may have his or her entire genome stolen. Even worse, that data in the wrong hands can do unthinkable harm. This Note explains how this industry trades genetic data like any other commodity, and how current laws do not regulate the DTC genetic testing industry to an appropriate extent. It then argues that this industry must be regulated to protect its consumers. This Note proposes a federal law with a two-part solution. First, customers who

* J.D. Candidate, 2022, Drexel University Thomas R. Kline School of Law. I would like to thank Professor Robert Field for all the helpful insights, critiques, and encouragement. I would also like to thank my parents for always supporting me in all that I do. Without them, none of this would be possible.

experience harm as a result of a genetic data breach must be permitted to seek recovery for such harms, regardless of whether the DTC genetic testing industry was negligent. Second, this industry must be regulated by incentivizing appropriate security and deterring subpar security practices.

TABLE OF CONTENTS

INTRODUCTION

Deoxyribonucleic acid (DNA) was first identified by Swiss chemist Friedrich Miescher in the 1860s, where he identified "nuclein" within "the nucleus of white blood cells."[1] Nearly a century later, in 1953, James Watson and Francis Crick, with help from Rosalind Franklin and Maurice Wilkins, discovered the DNA double helix.[2] This discovery led to modern molecular biology, where insights into the genetic code and protein synthesis have led to the current, multi-billion dollar biotechnology industry.[3] One of the greatest advances derived from the work of Watson and Crick is human genome mapping,[4] which entered the spotlight with the onset of the Human Genome Project (HGP) on October 1, 1990.[5]

One market that has capitalized on the human genome is the direct-to-consumer (DTC) genetic testing market.[6] The two

1. Leslie A. Pray, *Discovery of DNA Structure and Function: Watson and Crick*, SCITABLE (2008), https://www.nature.com/scitable/topicpage/discovery-of-dna-structure-and-function-watson-397/.

2. *Id.*

3. Nat'l Insts. of Health, *The Discovery of the Double Helix*, 1951–1953, U.S. NAT'L LIBR. OF MED., https://profiles.nlm.nih.gov/spotlight/sc/feature/doublehelix (last visited Aug. 31, 2021).

4. *Id.*

5. Nat'l Insts. of Health, *Human Genome Project Timeline of Events*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/human-genome-project/Timeline-of-Events (Feb. 12, 2021).

6. *See* BIS Rsch., *Global Direct-to-Consumer Genetic Testing Market to Reach $6.36 Billion by 2028*, CISION PR NEWSWIRE (May 21, 2019, 9:30 AM), https://www.prnewswire.com/news-releases/global-direct-to-consumer-genetic-testing-market-to-reach-6-36-billion-by-2028—300853946.html (noting that two factors driving demand in this space are "increased growing awareness among consumers regarding the genomic testing"
services and growing curiosity regarding genomic information that is then "used to assess [a person's] lineage and health-related genetic predispositions").

biggest players in this market are 23andMe, providing over nine million tests since its inception, and Ancestry, providing over fourteen million tests.[7] It should not be mistaken—these are for-profit businesses.[8] As this market grows, so too does concern over genetic data privacy grow.[9] These companies are not simply dealing with data regarding the websites a person likes to visit; instead, they are dealing with data comprising a person's genetic code—the most precious type of immutable data. Companies like 23andMe protect genetic data through de-identification and aggregation of that data.[10] However, this method is not as secure as one may think. Studies show that de-identified data can be re-identified with increasing ease.[11] Re-identification can harm DTC genetic testing customers in innumerable ways, but current laws do little to protect customers or punish DTC genetic testing companies in the event of a data breach or harm to customers.[12]

7. Antonio Regalado, *More than 26 Million People Have Taken an At-Home Ancestry Test*, MIT TECH. REV. (Feb. 11, 2019), https://www.technologyreview.com/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/.

8. Biz Carson & Kathleen Chaykowski, *Live Long and Prosper: How Anne Wojcicki's 23andMe Will Mine Its Giant DNA Database for Health and Wealth*, FORBES (June 6, 2019, 6:00 AM), https://www.forbes.com/sites/bizcarson/2019/06/06/23andme-dna-test-anne-wojcicki-prevention-plans-drug-development/#1abad1c6494d. For instance, 23andMe is valued at $2.5 billion by investors and, in 2018, the pharmaceutical giant GSK invested $300 million into 23andMe in return for an exclusive partnership to use 23andMe's massive genetic library to develop drugs. *Id.*

9. *See* Jason Chung, Aaron Kaufman, & Brianna Rauenzahn, *Privacy Problems in the Genetic Testing Industry*, THE REG. REV. (Jan. 23, 2021), https://www.theregreview.org/2021/01/23/saturday-seminar-privacy-problems-genetic-testing/ ("The rise of genetic testing has also raised genetic data privacy concerns. In the absence of more comprehensive state or federal regulations, DTC genetic testing companies enjoy significant autonomy to decide how to collect, store, and share consumer data."); *see also* Linnea I. Laestadius, Jennifer R. Rich & Paul L. Auer, *All Your Data (Effectively) Belong to Us: Data Practices Among Direct-to-Consumer Genetic Testing Firms*, 19 GENETICS MED. 513, 513 (2017), https://www.nature.com/articles/gim2016136.pdf ("[The] analysis shows that DTC-GT companies do not consistently meet international transparency guidelines related to confidentiality, privacy, and secondary use of data.").

10. *See Full Privacy Statement*, 23ANDME, https://www.23andme.com/about/privacy/#full-privacy-statement (Oct. 30, 2020) [hereinafter *Privacy Statement*].

11. *See infra* Section II.B.

12. *See* Chung et al., *supra* note 9.

DTC genetic testing companies generate significant profits from customers' genetic data and associated information and fall outside most federal laws regulating genetic data.[13] As such, a federal statute should be enacted that recognizes and compensates customers, holds companies accountable for breaches, and incentivizes data security. Part I of this Note provides background on the genetic testing market, describes the terms of service and privacy policy of a major DTC genetic testing company, and offers a few examples of the value of genetic data to these companies. Part II discusses the policies of consent, de-identification, and the growing ease of international laws that have the potential to, but do not, regulate DTC genetic testing companies. Part IV details why fault-based torts are not optimal to protect customers. Finally, Part V offers a solution to regulate this market and provide customers with needed safeguards.

I. THE DTC GENETIC TESTING MARKET AND ITS TERMS OF SERVICE

A. *The Evolution of Genetics and the DTC Genetic Testing Market*

Long before the HGP was underway, researchers capitalized on genetic engineering of microorganisms, which is what occurred in *Diamond v. Chakrabarty*.[14] In *Chakrabarty*, a microbiologist created and patented a microorganism "capable of breaking down multiple components of crude oil," which was intended to aid in the cleanup of oil spills.[15] The Supreme Court held that the microorganism was patent eligible because it was a man-made composition of matter, not an unpatentable product of nature.[16] Thus, the patent holder now had a twenty-year monopoly on the microorganism and could monetize it.[17]

13. *See infra* Sections I.A, II.A.
14. *See* Diamond v. Chakrabarty, 447 U.S. 303, 305–06 (1980).
15. *Id.* at 305.
16. *Id.* at 309.
17. *See* 35 U.S.C.A. § 154(a)(1)–(2) (West 2020).

In a more recent case, Myriad Genetics sought a patent on the DNA code that directs a cell to produce BRCA1 amino acids in what was essentially an attempt to patent the BRCA1 gene.[18] Myriad also sought to patent complementary DNA (cDNA) exons in the BRCA1 gene.[19] The Supreme Court held that the BRCA1 gene was not patent eligible because it was a product of nature.[20] However, it also held that the BRCA1 cDNA strand was patent eligible because, like the microorganism in *Chakrabarty*, cDNA was not a product of nature.[21] These two cases highlight the idea that genetically engineered organisms and manipulated genetic components are patent eligible and therefore can be monetized. The broader implication is that biomedical and biotechnological companies can monetize their products and services, but in order to create the product, access to the human genome is necessary.

The HGP decoded the human genome by determining the order, or "sequence," of the bases within DNA.[22] This process created maps that revealed the locations of genes on chromosomes and also created additional linkage maps that track inherited traits over generations.[23] The HGP has been critical, for instance, to advance the study of rare genomic diseases and to guide medical treatments for common

18. Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576, 584 (2013). While the BRCA1 and BRCA2 genes are meant to "protect you from getting certain cancers," they are also "the genes most commonly affected in hereditary breast and ovarian cancer." *Genetic Testing for Hereditary Breast and Ovarian Cancer*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/genomics/disease/breast_ovarian_cancer/testing.htm (last visited Aug. 31, 2021).

19. *Myriad Genetics*, 569 U.S. at 584–85. cDNA is defined as "a DNA that is complementary to a given RNA which serves as a template for synthesis of the DNA." *cDNA*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/cDNA (last visited Aug. 28, 2021). cDNA is either produced by certain forms of virus or is synthesized in a laboratory. *cDNA vs Genomic DNA*, BIOCHAIN, https://www.biochain.com/general/cdna-vs-genomic-dna/ (last visited Aug. 28, 2021).

20. *Myriad Genetics*, 569 U.S. at 576.

21. *Id.* at 576, 590–91.

22. Nat'l Insts. of Health, *What Is the Human Genome Project?*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/human-genome-project/What (Oct. 28, 2018).

23. *Id.*

diseases.[24] Through research that built upon the work of the HGP, researchers have discovered that most diseases have some genetic component associated with them, whether that genetic component is inherited or acquired by genetic mutation.[25] This realization holds many implications, one of which is the ability to monetize peoples' curiosity concerning their genomes. In a 2008 study, researchers found that 84% of 4,569 adults surveyed supported the idea of a study looking at the interactions between genes, environment, and lifestyle.[26] Additionally, 60% reported they would be likely willing to submit their own DNA for the study.[27] This public curiosity presents a blank check for those looking to capitalize on genetics.

DTC genetic testing started in 1996.[28] Although DTC genetic testing was not initially a booming industry, "[a]s many people purchased consumer DNA tests in 2018 as in all previous years combined."[29] To quantify that figure, twenty-six million consumers added their DNA to one of four leading DTC genetic testing companies from 1996 through the start of 2019.[30] Additionally, research institutions and pharmaceutical companies continue to utilize these DTC genetic testing

24. Nat'l Insts. of Health, *Human Genome Project Produces Many Benefits*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/27549135/nov-2011-human-genome-project-produces-many-benefits (June 11, 2012) (describing how genomic research has guided treatments for specific types of blood thinners where certain blood thinners prove ineffective for people who carry specific genetic variants).

25. Nat'l Insts. of Health, *Genetic Disorders*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/For-Patients-and-Families/Genetic-Disorders (May 18, 2018).

26. Johns Hopkins Univ., *Survey Finds Wide Public Support for Nationwide Study of Genes, Environment and Lifestyle*, SCIENCEDAILY (Nov. 12, 2008), https://www.sciencedaily.com/releases/2008/11/081112160848.htm.

27. *Id.*

28. Scott Bowen & Muin J. Khoury, *Consumer Genetic Testing Is Booming: But What Are the Benefits and Harms to Individuals and Populations?*, CTRS. FOR DISEASE CONTROL & PREVENTION (June 12, 2018), https://blogs.cdc.gov/genomics/2018/06/12/consumer-genetic-testing/.

29. Regalado, *supra* note 7.

30. *Id.*

company's DNA libraries as gene therapies are broadened to cover more types of diseases and other genetic traits.[31]

Genetic data has immense secondary value, from uses in research to uses in advertising, yet many DTC genetic testing companies are not explicit regarding whether it is the customer or the company that retains the rights to, and derives profits from, commercialization of genetic information.[32] One study found that 73%—forty out of fifty-five—of DTC genetic testing policies also "did not explicitly address ownership of genetic material or the resulting data," and that those policies did not "discuss licensing or commercialization of that [genetic data]."[33] However, 18% of companies—ten out of fifty-five—stated that the company retained the sole right to commercialization of customers' genetic data, and nine of those ten also stated that consumers would receive no personal benefit from commercialization.[34] Of the 13% of companies—seven out of fifty-five—that stated customers "retained ownership of their genetic material," five of those companies still reserve the rights to any commercialization and licensing of any product derived from customers' genetic material.[35] It is therefore clear that DTC genetic testing companies overwhelmingly seek to profit from licensing and commercializing consumers' genetic data and associated information. Some of these companies collect substantial amounts of customer data, both personal and genetic, including "genomic sequence, name, self-disclosed family history, health conditions, race, ethnicity, sexual

31. *See, e.g.*, Lydia Ramsey Pflanzer, *Why Pharma Giant GSK Just Made a $300 Million Bet on 23andMe's Approach to Finding New Medicines*, BUS. INSIDER (July 25, 2018, 11:21 PM), https://www.businessinsider.com/why-gsk-invested-300-million-in-23andme-genetic-drug-discovery-collaboration-2018-7.

32. 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, 52–53 (2018).

33. *Id.* at 52. This study further found that 39% of companies–thirty-five out of ninety–surveyed had no accessible policy discussing "how genetic data was collected, used, or shared." *Id.* at 48.

34. *Id.* at 52.

35. *Id.* at 52–53.

orientation, age, social networks, place of employment, . . . photos, and real-time tracking of [customers'] geographic location."[36] One board member of 23andMe remarked, "[t]he long game here is not to make money selling kits, although the kits are essential to get the base level data."[37] As one critic put it, "[t]he product really isn't really a kit, . . . the product is you."[38]

As the 23andMe board member's remark shows, data collection is the central and fundamental business strategy of these companies.[39] Marketing data to pharmaceutical companies is a prime example. According to one researcher, "23andMe . . . made around $130 million from selling access to about [one] million genotypes, . . . implying [that the] average price [per genotype is] around $130."[40] A concrete example of the value 23andMe derives from genetic data is that of its deal with GlaxoSmithKline (GSK), where GSK paid $300 million for access to customers' genetic data for new drug development.[41] Moreover, on June 17, 2021, 23andMe went public after a merger connected to Richard Branson.[42] On its first day as a

36. Katherine Drabiak, *Caveat Emptor: How the Intersection of Big Data and Consumer Genomics Exponentially Increases Informational Privacy Risks*, 27 HEALTH MATRIX 143, 159 (2017); see also *id.* at 52.

37. Sara Chodosh, *Getting Your Genetic Disease Risks from 23andMe Is Probably a Terrible Idea*, POPULAR SCI. (Apr. 7, 2017, 8:33 PM), https://www.popsci.com/23andme-is-probably-terrible-idea/.

38. *Id.*

39. *See id.*

40. Ben Hirschler, *Cashing In on DNA: Race On to Unlock Value in Genetic Data*, REUTERS, https://www.reuters.com/article/us-health-dna/cashing-in-on-dna-race-on-to-unlock-value-in-genetic-data-idUSKBN1KO0XC (Aug. 3, 2018, 4:01 AM). On the other hand, most personal data, like age, gender, and location are worth fractions of a penny per person. Emily Steel, Callum Locke, Emily Cadman, & Ben Freese, *How Much Is Your Personal Data Worth?*, FIN. TIMES, (June 12, 2013), https://ig.ft.com/how-much-is-your-personal-data-worth/.

41. Pflanzer, *supra* note 31.

42. Enrique Dans, *23andMe: Genetics Goes Public*, FORBES (June 20, 2021, 9:11 AM), https://www.forbes.com/sites/enriquedans/2021/06/20/23andme-genetics-goespublic/.

publicly traded company, the share price rose 20%,[43] highlighting market interest in genetic testing.[44]

23andMe is not alone in the mergers and acquisitions space. Amgen, an American pharmaceutical company, acquired deCODE Genetics for $415 million, which included deCODE's genetic data on Icelanders that traced back generations.[45] GSK also made a similar acquisition of Human Genome Sciences for approximately $3 billion.[46] In its privacy statement, 23andMe cautions that in the event of a merger or acquisition by another company, a customer's personal information will likely be among the assets transferred.[47]

The above are only a few examples of the prominent instances of the high value of genetic data and how it is bought and sold like any other commodity. Buying and selling data will only increase as new applications for that data are discovered.[48] Unless legal measures are enacted to regulate this industry and protect customers and their data, DTC genetic testing companies may have less of an incentive to secure their data libraries, and, as a result, customers are more likely to experience harm.

43. Connie Lin, *23andMe Jumps on Stock Market Debut, As Privacy Concerns About Genetic Testing Abound*, FAST CO. (June 17, 2021), https://www.fastcompany.com/90648289/23andme-jumps-on-stock-market-debut-as-privacy-concerns-about-genetic-testing-abound.

44. Dans, *supra* note 42.

45. Meg Tirrell, *Iceland's Genetic Goldmine, and the Man Behind It*, CNBC, https://www.cnbc.com/2017/04/06/icelands-genetic-goldmine-and-the-man-behind-it.html (Apr. 6, 2017, 4:21PM).

46. Michael J. de la Merced, *Glaxo to Buy Human Genome Sciences for $3 Billion*, N.Y. TIMES (July 15, 2012, 6:07 PM), https://dealbook.nytimes.com/2012/07/15/glaxosmithkline-in-talks-to-buy-human-genome/.

47. *Privacy Statement*, *supra* note 10.

48. *See, e.g.*, Reuters Staff, *Bad Driver? Blame Your Genes*, REUTERS (Oct. 29, 2009, 12:35AM), https://www.reuters.com/article/us-genes-driving/bad-driver-blame-your-genes-idUSTRE59S0M720091029 (describing the correlation between genetics and driving ability); Sarah Zhang, *How a Genealogy Website Led to the Alleged Golden State Killer*, THE ATLANTIC, https://www.theatlantic.com/science/archive/2018/04/golden-state-killer-east-area-rapist-dna-genealogy/559070/ (Apr. 27, 12:45 PM) (describing how the notorious Golden State Killer was caught when DNA from crime scenes were matched with DNA from the killer's relative on the open-source genealogy website GEDmatch).

B. 23andMe's Privacy Statement

In terms of number of kits sold, 23andMe is one of the two major DTC genetic testing companies in the United States.[49] As a result, it will be the primary focus here. To understand the broad scope of information that DTC genetic testing companies gather, it is helpful to start with the information they collect from customers. 23andMe's privacy statement provides two relevant categories of information it collects.

First, 23andMe collects the information a customer provides directly to the company.[50] Within this category, 23andMe collects registration information and self-reported information.[51] Registration information includes a customer's name, date of birth, address, and other contact information.[52] The customer also has the option to provide self-reported information.[53] This may include information like eye color, height, ethnicity, disease, and other health-related information, like cholesterol levels and visual acuity, as well as family history information.[54]

Second, 23andMe collects information related to its genetic testing services.[55] This category includes a customer's saliva sample and genetic information.[56] A customer's genetic information is derived from his or her saliva sample by means of extracting the customer's DNA from the sample.[57] Genetic information are the results reported to the customer.[58] In other words, it is the customer's unique genome sequence that

49. *See* Regalado, *supra* note 7.

50. *See Privacy Statement*, *supra* note 10.

51. *Id.*

52. *Id.*

53. *Id.*

54. *Id.* Family history information is "information similar to the foregoing about [a customer's] family members. *Id.* This section also provides warning that a customer should get permission from family members prior to disclosing familial information. *Id.*

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

23andMe is paid to generate, which may also entail health or ancestry reports.[59]

Under the terms of its privacy policy, 23andMe provides a "meaningful choice" to its customers, ensuring that "[the customer] decide[s] how [his or her] information is used and with whom it is shared."[60] 23andMe destroys a customer's saliva sample and DNA after analysis unless the customer consents to sample storage and additional analyses.[61] However, a customer's genetic information is retained by 23andMe and may be used for other purposes.[62] A customer may initially opt-in and consent to have his or her genetic data and other personal information, excluding registration information, used for research.[63] The privacy statement goes on to provide that "23andMe [r]esearch may be sponsored by, conducted on behalf of, or in collaboration with third parties, such as non-profit foundations, academic institutions or pharmaceutical companies."[64]

Customer data, including genetic data, shared with third parties "will be summarized across enough customers to minimize the chance that . . . personal information will be exposed."[65] Individual-level data will not be disseminated to third parties without a customer's explicit consent.[66] If a customer does initially consent to research, his or her genetic information and self-reported information will be shared with third parties, but that information will first be de-identified.[67]

59. *Id.*

60. *Your Privacy Comes First*,

23ANDME, https://www.23andme.com/privacy/ (last visited Sept. 7, 2021) [hereinafter *Your Privacy Comes First*].

61. *Privacy Statement*, *supra* note 10.

62. *See id.*

63. *Id.*; *Research Consent Document*,

23andMe, https://www.23andme.com/about/consent/ (last visited Sept. 7, 2021) [hereinafter *Research Consent Document*].

64. *Privacy Statement*, *supra* note 10.

65. *Research Consent Document*, *supra* note 63.

66. *Your Privacy Comes First*, *supra* note 60.

67. *See Privacy Statement*, *supra* note 10.

23andMe defines de-identified information as "information that has been stripped of [a customer's] . . . identifying data such that [the customer] cannot reasonably be identified as an individual."[68] Like de-identified information, aggregated information will be disseminated to third parties under the customer's initial consent, but consent here is not required.[69] Aggregated information is "information that has been combined with that of other users and analyzed or evaluated as a whole, such that no specific individual may be reasonably identified."[70]

It is clear that 23andMe does obtain initial consent from any customer by an opt-in agreement before the customer's information is disseminated to third parties.[71] It is also clear that the information will be de-identified before it is disseminated.[72] However, de-identification is imperfect as a mode of protection for genetic and self-reported data because re-identification by bad actors is undoubtedly possible.[73] Because the de-identification mode of protection is imperfect, other forms of protection must exist to limit the chances of breaches and re-identification to the greatest extent possible.

C. *23andMe's Terms of Service*

23andMe permits its customers to request that their personal information be deleted and not used in future research

68. *Id.*

69. *See Your Privacy Comes First*, *supra* note 60.

70. *Privacy Statement*, *supra* note 10.

71. *Privacy Highlights*, 23ANDME, https://www.23andme.com/about/privacy/#full-privacy-statement (Oct. 30, 2020) ("23andMe will not sell, lease, or rent your individual-level information to a third party for research purposes without your explicit consent."); *see also Privacy Statement*, *supra* note 10 ("Your De-identified Genetic and Self-Reported Information may be used for 23andMe Research only if you have consented to this use by completing a Consent Document.").

72. *See Privacy Statement*, *supra* note 10 (stating that a customer's genetic and self-reported information will be used for research, but that it will first be de-identified).

73. *See infra* Section II.B (discussing studies that confirm the growing ease of re-identifying de-identified data).

projects.[74] However, an overwhelming majority of customers consent to 23andMe using their data.[75] For instance, 80% of 23andMe's customers have consented to have their data used by third parties.[76] This overwhelming percentage begs the question: are customers fully informed of the scope of their consent? It is interesting that 80% of customers are supposedly aware that 23andMe's terms of service require that customers waive any property right to research or commercial products developed from their data.[77] It is even more interesting that 80% of customers are aware that sharing genetic information with others "could be used against [their] interests."[78]

Another concerning aspect for customers is that 23andMe, at its sole discretion and without prior notice, may change or revoke aspects of its services at any time.[79] More importantly, 23andMe may unilaterally change its terms of service or privacy statement at any time.[80] The company does not ensure that a customer will be notified directly of material changes; rather, it may give notice thirty days prior to enactment by posting the to-be-adopted changes on its website and simply recommends that a customer revisit the website "periodically to stay aware of any changes" to its policies.[81] Like other standard agreements, a customer's continued use of services after changes are implemented acts as an agreement to those

74. *See Terms of Service*, 23ANDME, https://www.23andme.com/about/tos/ (Sept. 30, 2019) [hereinafter *Terms of Service*].

75. *23andMe Research Innovation Collaborations Program*, 23ANDME, https://research.23andme.com/research-innovation-collaborations/ (last visited Aug. 25, 2021).

76. *Id.* ("The 23andMe database is a rich resource, with genotypic and phenotypic information from more than 5 million of [23andMe's] customers, 80 percent of whom consent to participate in 23andMe Research.").

77. *See Terms of Service*, *supra* note 74.

78. *Id.*

79. *See id.*

80. *See id.* (stating that 23andMe may change its terms of service, and that a customer is held to have acknowledged and agreed to the changes if the customer continues to use the services after the date on which the terms were changed); *see also* Privacy Statement, *supra* note 10 (stating nearly identical language to that in the terms of service).

81. *Terms of Service*, *supra* note 74; *Privacy Statement*, *supra* note 10.

changes.[82] If a customer disagrees with any changes, that customer's only recourse is to stop using 23andMe's services and to delete his or her account.[83] However, it remains unclear what happens to that customer's genetic information if it is already part of research or third-party use.

II. ATTEMPTS TO PROTECT DATA: DE-IDENTIFICATION AND RE-IDENTIFICATION

Part I displays the lucrative nature of genetic testing. It also shows, in a broad sense, how 23andMe attempts to assure customers that it is protecting their data, and how 23andMe can change its protections without giving customers much notice. This Part examines the two primary methods of data protection used by 23andMe. Section A details de-identification and its use to get around consent, and Section B turns its focus to re-identification and the growing concerns around this technique as a protective measure.

A. *Consent and De-Identification*

De-identifying customer data is central to 23andMe's business scheme.[84] Entities that deal with sensitive patient data, like genetic data, may share this data with third parties if the entity obtains consent or de-identifies the data.[85] While

82. *Terms of Service*, *supra* note 74; *Privacy Statement*, *supra* note 10. 23andMe offers two different types of services. *See Choose the Service That's Right for YOU*, 23ANDME, https://www.23andme.com/compare-dna-tests/ (last visited Aug. 31, 2021). One type of service provides the customers with ancestry reports. *Id.* Another provides the customer with ancestry and health reports. *Id.* A customer may also add, a la carte, health predispositions, genetic trait carrier reports, and wellness reports to some packages. *Id.* Finally, 23andMe recommends customers purchase the 23andMe Membership, which allows customers to add other packages, such as enhanced features that allow a customer to find distant relatives and attain ongoing new reports periodically. *Id.*

83. *See Terms of Service*, *supra* note 74; *Privacy Statement*, *supra* note 10.

84. *See Individual Data Sharing Consent*, 23ANDME, https://www.23andme.com/about/individual-data-consent/ (last visited Aug. 31, 2021) [hereinafter *Individual Data Sharing Consent*].

85. Khaled El Emam, Sam Rodgers & Bradley Malin, *Anonymising and Sharing Individual Patient Data*, 350 BRIT. MED. J. 1, 1 (2015) (stating that "[t]here are two legal mechanisms that

23andMe obtains initial consent from its customers to participate in research and have their data de-identified, no subsequent consent is obtained for each use of de-identified data by a third party.[86]

To some researchers, it is impractical to rely on consent.[87] If medical data are obtained in one context and then used for a subsequent purpose, consent is often not obtained for that subsequent purpose because it is not practical to attempt to obtain consent from a large number of people whose data will be used for that subsequent purpose.[88] Consider the following hypothetical. If genetic data is obtained by 23andMe for customer genetic testing purposes, and then that genetic data is used by a pharmaceutical manufacturer for research to develop a new class of drug, renewed consent is not obtained by 23andMe from the customer for the purpose of disseminating that data to the pharmaceutical manufacturer because it would be too much of a hassle to obtain consent from every customer in a cohort before handing that data over to the pharmaceutical manufacturer.

Moreover, when a cohort must consent to have their data used for secondary purposes, it often leads to representative skews in the cohort and can hinder medical research.[89] To one

would permit data custodians [like 23andMe] to share patient data for secondary purposes . . . (a) consent and (b) anonymisation.").

86. *See Individual Data Sharing Consent*, *supra* note 84. However, "there is evidence that many research ethics boards will permit the sharing of patient data without consent for research purposes if it is [anonymized]." El Emam et al., *supra* note 85.

87. *See id.* Obtaining consent for each subsequent use is impractical because re-contacting patients for consent is too burdensome. *Id.* Further, there is evidence that by attaining consent for each use, it creates a consent bias in study participants. *Id.*

88. *Id.*

89. Michelle E. Kho, Mark Duffett, Donald J. Willison, Deborah J. Cook & Melissa C. Brouwers, *Written Informed Consent and Selection Bias in Observational Studies Using Medical Records: Systematic Review*, 338 BRIT. MED. J., Mar. 12, 2009, at 1 ("Significant differences between participants and non-participants may threaten the validity of results from observational studies that require consent for use of data from medical records."). However, 23andMe may be distinguishable from the conclusions of this study because the study reported that 66.9% of participants consented to data use, whereas 80% of 23andMe customers consent. *See id.*; *see also* Jorge L. Contreras, *Genetic Property*, 105 GEO. L.J. 1, 6 (2016) (noting that, with informed consent requirements, "individuals have brought litigation asserting . . . control over the use

author, "it appears that the mechanism of informed consent for data-based research may be broken beyond repair."[90] This is because obtaining consent for data use from millions of participants is "daunting"[91] and can lead to massive lawsuits when the data is used for purposes that were not expressed in the consent agreement.[92] Therefore, de-identifying data may be a much more attractive option to entities like 23andMe because it avoids the issues of obtaining proper consent.

De-identified data is subject to less regulation than data that contains identifiers.[93] Unlike identifiable data, de-identified data in the United States and Europe is not covered by privacy laws, which allows entities like 23andMe to use this data without consent for any secondary purpose, like selling it to a pharmaceutical company.[94] Thus, it is advisable for any entity engaging in research and other data transfers to de-identify that data to avoid the issue accompanying consent. From the customer's perspective, though, concerns should still arise because what constitutes de-identified data is unclear.[95]

For instance, the Health Insurance Portability and Accountability Act (HIPAA) states that de-identified data is "[h]ealth information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual."[96] It is

of data that is obtained from their genetic material, [thus] hindering ongoing scientific research.").

90. Contreras, *supra* note 89, at 36.

91. *See id.* However, this article references consent in the context of a property right to data, which is distinguishable from the consent discussed in this Note because a property right for data is not advocated for here. *See id.* at 4*; see also* discussion *infra* Part IV.

92. *See, e.g.*, Havasupai Tribe v. Ariz. Bd. of Regents, 204 P.3d 1063, 1070 (Ariz. Ct. App. 2008). For example, in *Havasupai Tribe v. Arizona Board of Regents*, plaintiffs requested that defendants pay ten million dollars for improper data usage. *Id.*

93. Benjamin T. Van Meter, *Demanding Trust in the Private Genetic Data Market*, 105 CORNELL L. REV. 1527, 1529–30 (2020); El Emam et al., *supra* note 85, at 1.

94. *See* El Emam et al., *supra* note 85, at 1 (stating that the United States and Europe "do not designate anonymized health data as personal information" and therefore such data is not covered by privacy laws).

95. *See* Van Meter, *supra* note 93, at 1530.

96. El Emam et al., *supra* note 85, at 1.

clear that de-identified information is information that cannot reasonably identify the individual from which the information is derived. But what remains ambiguous is what constitutes a "reasonable basis," which creates inconsistent de-identification practices for health data.[97] In theory, de-identification practices from one DTC genetic testing company may not be identical to the practices of another DTC genetic testing company, or even the practices of a healthcare system.

Nonetheless, standards and guidelines do exist that divide certain variables, like the variables discussed *supra* in Part I, Section B,[98] into two groups: direct identifiers and quasi-identifiers.[99] Direct identifiers are defined as "features that permit direct recognition [of] . . . individuals, such as personal names, email addresses, telephone numbers, and social insurance numbers.."[100] Quasi-identifiers, on the other hand, "are features that can indirectly identify individuals, such as their date of birth, death, or clinic visit, residence postal code, and ethnicity, . . . [as well as] demographics and socioeconomic information."[101] Both direct identifiers and quasi-identifiers must be addressed in the de-identification process.[102] But removing too much information from a data set perturbs the set and renders its utility minimal for research purposes.[103] Thus, there must be a balance of privacy protection and utility within data sets, and guidelines have set a probability range for re-identification for public and non-public databases.[104] The probability of re-identification generally must be between 0.05 and 0.33, thus recognizing that the probability of re-identification can never be zero.[105] This could be why 23andMe

97. *Id.* ("Even the concept of anonymous or non-identifiable data is ambiguous.").

98. *See supra* Section I.B (listing variables, such as: name, date of birth, address, and other contact information).

99. El Emam et al., *supra* note 85, at 2.

100. *Id.*

101. *Id.*

102. *Id.*

103. *Id.* at 5.

104. *Id.* at 4–5.

105. *Id.* at 4; *see also* Van Meter, *supra* note 93, at 1530.

and HIPAA require protection of personal data such that a person cannot "reasonably" be identified.[106] Re-identification, though, may be a larger problem than was originally thought, further proving the need for increased customer protection.[107]

B. *Re-Identification*

Genetic data is one of the many forms of data vulnerable to re-identification.[108] Generally, re-identification occurs when identifying information is discoverable in de-identified data.[109] One way data can be re-identified is through insufficient de-identification, which "occurs when a direct or [quasi] . . . identifier inadvertently remains in a data set that is made available to the public."[110] Studies show that de-identified and aggregated datasets can be re-identified with greater likelihood than previously assumed.[111] A 2015 study, for example, developed an attack system that examined de-identified, aggregated data sets for cellphone users' triangulated, timestamped locations.[112] It found that the attack system could re-identify individuals with an accuracy of 73–91%.[113] The system was able to re-identify individuals because their mobility habits were unique such that the system could recognize data points belonging to a single person.[114] Like the unique, but variable, timestamped locations that made it easier

106. *See* El Eman et al., *supra* note 85, at 1.

107. *See* Van Meter, *supra* note 93, at 1533 ("Studies are increasingly showing that supposedly de-identified and aggregated datasets are more amenable to re-identification than previously thought").

108. *Id.* at 1548.

109. Boris Lubarsky, Note, *Re-Identification of "Anonymized Data,"* 1 GEO. L. TECH. REV. 202, 208 (2017).

110. *Id.* at 209.

111. Van Meter, *supra* note 93, at 1533; *see generally* FENGLI XU, PENGYU ZHANG, ZHEN TU, XIAOMING FU, YONG LI & DEPENG JIN, TRAJECTORY RECOVERY FROM ASH: USER PRIVACY IS NOT PRESERVED IN AGGREGATED MOBILITY DATA (2017) (proving that publishing aggregated mobility data could lead to a privacy breach in individuals' trajectories by conducting experiments on two real-world datasets).

112. XU ET AL., *supra* note 111, at 2.

113. *Id.*

114. *Id.* at 1241; *see also* Van Meter, *supra* note 93, at 1533.

to identify an individual, genetic data is immutable, meaning that an individual can be identified by his or her genetic data similar to the way the attack system identified individuals by unique mobility habits.[115]

Quasi-identifiers that remain in insufficiently de-identified data, like residential postal codes, can also be used to re-identify individuals.[116] In one study, researchers had an 85% success rate of re-identifying children in a birth registry using only the mother's date of birth and postal code.[117] To conduct this study, researchers used the BORN registry as an example dataset.[118] BORN is a de-identified registry for births that occur in Ontario, and it is used and disclosed for research and public health purposes, similar to the uses of 23andMe.[119] In this study, the researches had no direct information on the child, yet the probability of re-identification was still high.[120] This draws parallels to a situation where a mother gets a DTC genetic test, but it is her child who could still be identified with high probability, though the child's genome was never sequenced.[121] Moreover, using the mother's date of birth, the child's date of birth, and the child's sex, researchers found there was a 91% chance of re-identification of the child. [122] Therefore, even datasets that only contain a couple quasi-identifiers can prove sufficient to re-identify an individual. [123]

The risk of re-identification persists because the complete anonymization of genetic data is likely impossible since a person's genome is inherently identifying.[124] For instance, a study performed by a geneticist at the Whitehead Institute for

115. *See* Van Meter, *supra* note 93, at 1533; Xu et al., *supra* note 111, at 1243.
116. *See* El Emam et al., *supra* note 85, at 2.
117. *Id.* at 3.
118. *Id.* at 1.
119. *See id.*
120. *See id* at 3.
121. *See id.*; Chung et al., *supra* note 9.
122. El Emam et al., *supra* note 85, at 3.
123. *See id.*
124. *See* Contreras, *supra* note 89, at 34.

Biomedical Research found that an anonymous male donor's identity could be discovered from a genetic database using only a partial Y chromosome sequence, his age, and his state of residence.[125] Re-identification is plausible in many instances using few data points, and genetic data cannot be unduly broken down as it loses its utility for research purposes.[126] Given this tug-of-war between privacy and research, even 23andMe cofounder Linda Avey stated, "it's a fallacy to think that genomic data can be fully anonymized."[127] If these companies admit that the data they collect will never be truly anonymous, this provides another strong basis to require robust security standards to safeguard customers to the fullest extent possible.

III. CURRENT STATUTORY PROTECTIONS SURROUNDING GENETIC DATA

Data privacy, including genetic data privacy, in the United States is composed of piecemeal protections derived from common law, constitutional law, and state and federal regulation.[128] Additionally, "[m]ost data collected commercially in the United States [does not per se have] protection under the law."[129] Federal and state legislators single out specific types of

125. John Bohannon, *Genealogy Databases Enable Naming of Anonymous DNA Donors*, 339 SCI. 262, 262 (2013).

126. *See* El Emam et al., *supra* note 85, at 3–4.

127. 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/?sh=aa5e1141bba5. If a person or entity accessed these genetic databases, 60% of Americans of European descent can be identified, regardless of whether they have joined a service themselves. 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. Society is not far from a point where 90% of people can be identified through the DNA of their cousins in genealogical databases. *Id.* This is because researchers have found that only 2% of a target population must have done a DNA test to identify nearly everyone else in that population. *Id.*

128. Contreras, *supra note* 89, at 18.

129. John Wilbanks, *Portable Approaches to Informed Consent and Open Data*, *in* PRIVACY, BIG DATA, & THE PUBLIC GOOD 234, 235 (Julia Lane, Stefan Bender, & Helen Nissenbaum eds., 2014).

data to protect, with one prime example being protected health information that is regulated by HIPAA.[130] Data protections often turn on whether the entity collecting the data is covered under regulations like HIPAA and also whether the data is de-identified.[131] De-identification and aggregation techniques used by DTC genetic testing companies allow these companies to fall outside the regulatory scheme of some of the most important data privacy laws.[132] DTC genetic companies essentially tiptoe around more stringent regulations of their data.

This Part examines two categories of laws that are intended to protect people and their associated data. Section A details laws that concern data disclosure; for instance, when and how a data-holding entity may transfer or share data. Section B details laws that concern unauthorized data use; for instance, how an employer cannot deny a person a job on the basis of that person's genetic makeup.

A. *Laws Surrounding Unauthorized Data Disclosure*

1. The Common Rule

One of the most important forms of protection for research data is The Federal Policy for the Protection of Human Subjects, known otherwise as the "Common Rule," which was created in light of the National Research Act of 1974.[133] The Common Rule sets the standard for informed consent of human subjects in government-funded research.[134] It governs in situations where research is conducted on an "identifiable biospecimen," which

130. *See* 45 C.F.R. §§ 160, 164 (2021).

131. *See* Contreras, *supra* note 89, at 17, 33.

132. *See id.* at 17–18.; *see also* 45 C.F.R. § 164.514(a) (2013) (describing the standard protected health information); *see also Privacy Statement*, *supra* note 10 (describing 23andMe's use of aggregate information).

133. Robert I. Field, Anthony W. Orlando & Arnold J. Rosoff, *Am I My Cousin's Keeper? A Proposal to Protect Relatives of Genetic Database Subjects*, 18 IND. HEALTH L. REV. 1, 30 (2021) [hereinafter *Am I My Cousin's Keeper?*]; OFF. OF THE SEC'Y, U.S. DEP'T HEALTH, EDUC. & WELFARE, BELMONT REP. (1979), https://bit.ly/2VKZgQq.

134. *See* 45 C.F.R. § 46.109(b)–(c) (2021).

is a biospecimen for which the identity of the human subject may be readily ascertained.[135] Under its requirements, researchers must obtain written consent from potential research participants after disclosure of risks and benefits.[136] Further,:

[The] consent requirements for research involving identifiable data, biospecimens, and whole genome sequencing must [disclose] whether identifiers will be removed, whether biospecimens will be used for commercial purposes, whether the individual can expect to share in any profits, and whether clinically actionable results of genetic testing or genomic sequencing will be returned to the individual.[137]

The Rule requires that internal review boards (IRBs) enforce these protections by overseeing studies that utilize human subjects.[138] IRBs do this in two ways: by reviewing research plans and protocols before they are implemented and by reviewing ongoing research to enforce the required protections.[139] IRBs are only required when research is federally funded, or when research is used to support a new drug application to the Food and Drug Administration (FDA).[140]

Changes to the Common Rule were recently implemented.[141] Health and Human Services (HHS) proposed a change to the Common Rule to "extend coverage . . . to non-identifiable specimens."[142] However, non-identifiable biospecimens from human subjects were left out of the most recent Common Rule due to concerns over unnecessarily hindering research, among

135. 45 C.F.R. § 46.102(e)(6) (2021).

136. Leslie E. Wolf, Erin Fuse Brown, Ryan Kerr, Genevieve Razick, Gregory Tanner, Brett Duvall, Sakinah Jones, Jack Brackney & Tatiana Posada, *The Web of Legal Protections for Participants in Genomic Research*, 29 HEALTH MATRIX 1, 21–22 (2019) [hereinafter *Web of Legal Protections*].

137. *Id.* at 22; *see* Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149, 7256, 7266 (Jan. 19, 2017).

138. 45 C.F.R. § 46.101 (2021).

139. *Id.* § 46.109.

140. *Am I My Cousin's Keeper?*, *supra* note 133, at 31; *see* 45 C.F.R. § 46.101 (2020).

141. 49 C.F.R. pt. 11 (2021).

142. 45 C.F.R. §§ 46, 160, 164 (2021); *see also* Valerie Gutmann Koch & Kelly Todd, *Research Revolution or Status Quo?: The New Common Rule and Research Arising from Direct-to-Consumer Genetic Testing*, 56 HOUS. L. REV. 81, 106–07 (2018).

others.[143] Rather than increase protection for subjects, the 2018 revisions to the Rule eased restrictions on data use obtained for research.[144] One major change was that researchers could now obtain broad consent for various aspects of research, rather than individual consent for each aspect.[145] Moreover, IRB review is now not required when HIPAA applies, meaning if an investigator has obtained consent for data disclosure under HIPAA, any further review by an IRB is not required.[146] Further, genetic data does not fall under the umbrella of "human subject" if the specimen was not collected for a "currently proposed research project," and if investigators "cannot readily ascertain the identity of the individual(s) to whom the . . . specimens pertain."[147] DTC genetic testing companies like 23andMe that do not use government funding and that employ de-identification techniques are not subject to informed consent under the Common Rule.[148]

23andMe states that "much of" its policies regarding genetic data align with the Common Rule.[149] Specifically, it states that "[a]lthough technically only federally funded research has to meet [the Common Rule] standard, 23andMe voluntarily applies it to our own *internal* research."[150] 23andMe employs an external IRB to review and monitor its research.[151] It claims to have a team that ensures its research "follows the federal

143. Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149, 7165 (Jan. 19, 2017); *see also* Koch & Todd, *supra* note 142, at 107.

144. *Am I My Cousin's Keeper?*, *supra* note 133, at 30; *see also* 45 C.F.R. § 46.101(l)–(5) (2021).

145. *See* 49 C.F.R. § 11.116 (2021).

146. *How the Common Rule 2018 Updates Can Affect Your Research and Quality Improvement Strategies*, PROMETHEUS RSCH., https://www.prometheusresearch.com/common-rule-updates-2018/ (last visited Sept. 5, 2021). If data has been de-identified according to HIPAA regulations, the exception also applies. *Web of Legal Protections*, *supra* note 136, at 43–44.

147. *Coded Private Information or Specimens Use in Research, Guidance*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Oct. 16, 2008), https://www.hhs.gov/ohrp/regulations-and-policy/guidance/research-involving-coded-private-information/index.html.

148. Van Meter, *supra* note 93, at 1542–43.

149. *Protecting People in People Powered Research*, 23ANDME: 23ANDMEBLOG (July 30, 2014), https://blog.23andme.com/23andme-research/protecting-people-in-people-powered-research/ [hereinafter *Protecting People*].

150. *Id.* (emphasis added).

151. *Id.*

regulations and the instructions [of its] IRB."[152] However, the extent of IRB oversight to 23andMe data remains unclear.[153] Researchers using 23andMe datasets argued successfully to an IRB that their research did not involve "human subjects" under the Common Rule definition of the term.[154] 23andMe has even stated on its website that it prefers not to call users "human subjects"; rather, users are "people" or "partners in research."[155] This deliberate word choice by 23andMe affirms that 23andMe abides by the Common Rule regulations voluntarily; it is not required to abide under law, and it can revoke these voluntary protections unilaterally by its own choice.[156] Leaving it to a for-profit business to voluntarily self-regulate likely will not benefit the customer in the event of an issue arising over data protection.

2. The Privacy Rule

HIPAA provides baseline privacy and data security rules for the healthcare industry.[157] The Privacy Rule under HIPAA regulates the use and disclosure of an individual's "protected health information" by a "covered entity or business associate."[158] HIPAA covers genetic information, which includes the types of genetic tests that are used by DTC genetic testing companies.[159] However, the Privacy Rule covers only individually identifiable health information.[160] Under HIPAA,

152. *Id.*

153. *See, e.g.*, Nicholas Eriksson, J. Michael Macpherson, Joyce Y. Tung, Lawrence S. Hon, Brian Naughton, Serge Saxonov, Linda Avey, Anne Wojcicki, Itsik Pe'er & Joanna Mountain, *Web-Based, Participant-Driven Studies Yield Novel Genetic Associations for Common Traits*, 6 PLOS GENETICS 1, 16–17 (June 24, 2010).

154. *Id.* at 16.

155. *Protecting People*, *supra* note 149; Linda Avey, *It's Your Data . . . Shouldn't You Have Access to It?*, 23ANDME: 23ANDMEBLOG (June 22, 2009), https://blog.23andme.com/news/its-your-data-shouldnt-you-have-access-to-it/.

156. *See Protecting People*, *supra* note 149.

157. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996).

158. *See* 45 C.F.R. § 160.103 (2021).

159. *See id.*

160. *See id.*

individually identifiable health information is information that identifies an individual or information for "which there is a reasonable basis to believe [it could] be used to identify [an] individual."[161] Moreover, covered health information only includes individually identifiable information which "[i]s created or received by a health care provider, health plan, . . . employer, life insurer," and other similar entities.[162]

Generally, genetic data from DTC genetic testing companies fall outside HIPAA regulations.[163] DTC genetic testing companies are not considered covered entities for HIPAA purposes.[164] And these companies rely on de-identification and aggregation techniques such that their genetic data does not have a chance of "reasonabl[e]" re-identification,[165] despite growing studies to the contrary.[166] However, there exists an exception to this lack of HIPAA regulation when a company is considered a business associate of a HIPAA-covered entity. In other words, there is an exception to the general rule.[167] A DTC genetic testing company is considered a business associate under HIPAA only when it partners with a covered entity, which occurs when the genetic testing company handles the covered entity's patient data.[168] As the Privacy Rule is currently

161. *Id.*

162. *Id.*

163. Robert Gellman, U.S. DEP'T OF HEALTH & HUM. SERVS., HEALTH INFORMATION PRIVACY BEYOND HIPAA: A 2018 ENVIRONMENTAL SCAN OF MAJOR TRENDS AND CHALLENGES 2 (Dec. 13, 2017), https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf.

164. *See* 45 C.F.R. § 160.103 (2021).

165. *E.g., Privacy Statement*, *supra* note 10.

166. *See supra* Section II.B (discussing studies that confirm the growing ease of re-identifying de-identified data).

167. *See* 45 C.F.R. § 160.103 (2021) (defining business associate).

168. *Id.* For instance, 23andMe announced a partnership with Palomar Pomerado Health in 2009. *23andMe and Palomar Pomerado Health Partner to Give PPH Members Access to Their Genetic Information*, 23ANDME (Apr. 27, 2009), https://mediacenter.23andme.com/press-releases/23andme-and-palomar-pomerado-health-partner-to-give-pph-members-access-to-their-genetic-information/. In that situation, the members' genetic information generated by 23andMe would be subject to HIPAA's Privacy Rule because the data is from the health provider's patients, not 23andMe customers. § 160.103.

written, HIPAA does not otherwise apply to DTC genetic testing companies.

3. The European Union General Data Protection Regulation

The European Union (EU) has significantly more comprehensive privacy laws compared to the United States.[169] In 2016, the EU adopted the European Union General Data Protection Regulation (GDRP), which protects data of individuals unlike any federal law in the United States.[170] Under the GDPR, data subjects have rights to limit storage and use of their information that has been collected and stored electronically.[171] The Regulation applies to personal data, which includes anonymized genetic information, and it gives data subjects the right to access, transfer, or delete their data.[172] Companies must, '"by design and by default,' consider data protection," meaning a company must actively consider data protection with all new designs and activities.[173] Companies that are data controllers must report data breaches to their country's Data Protection Office within seventy-two hours of the breach.[174] Moreover, data controllers must conduct data protection impact assessments any time a controller begins a new project likely to involve "high risk" to peoples' personal

169. *See generally* Commission Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1 [hereinafter General Data Protection Regulation].

170. *See id.* at 35–36.

171. *Id.* (identifying the "storage limitation" to the GDPR).

172. *Id.* at 34–35; *What Is GDPR, the EU's New Data Protection Law?*, GDPR.EU, https://gdpr.eu/what-is-gdpr/ [hereinafter *What Is GDPR?*] (last visited Sept. 6, 2021) (providing a rundown of data subjects' privacy rights, including: the right to be informed, right of access, right to rectification, right to erasure, right to restrict processing, right to data portability, right to object, and rights in relation to automated decision making and profiling).

173. General Data Protection Regulation, *supra* note 169, at 15 (stating that, "by design and default," organizations must take data protection into consideration); *What Is GDPR?*, *supra* note 172.

174. General Data Protection Regulation, *supra* note 169, at 52; *What Does GDPR Stand for? (And Other Simple Questions Answered)*, GDRP.EU, https://gdpr.eu/what-does-it-stand-for/? [hereinafter *What Does GDPR Stand for?*] (last visited Sept. 6, 2021).

information.[175] These assessments are designed to address the risks of a project and to demonstrate compliance with GDPR.[176]

The GDPR applies to any company that collects or processes personal data on EU citizens, even if that company is not physically located within the EU.[177] Fines for violating the GDPR are significant. Specifically, penalties can reach a maximum of twenty million euros, or 4% of a company's global revenue, whichever is greater.[178] On top of those fines, data subjects can seek compensatory damages if the subject believes his or her data is being misused or transferred for unapproved purposes.[179] The United States does not have a comparable law, and though American companies are subject to the GDPR in Europe, the law does not provide for a cause of action in the United States.[180]

Though the GDPR is cutting edge for data protection laws, it is significantly limited in some respects. Its scheme requires that data subjects affirmatively assert their rights under the law, whereas an automatic-type cause of action would better serve

175. *See* General Data Protection Regulation, *supra* note 169, at 16; *Data Protection Impact Assessment (DPIA)*, GDRP.EU, https://gdpr.eu/data-protection-impact-assessment-template/ [hereinafter *DPIA*] (last visited Sept. 6, 2021).

176. General Data Protection Regulation, *supra* note 169, at 16; *see also* DPIA, *supra* note 175 ("[T]he GDPR requires DPIAs to contain . . . [a]n assessment of the risks to the rights and freedoms of data subjects.").

177. General Data Protection Regulation, *supra* note 169, at 33; *see also* DPIA, *supra* note 175 ("[I]f you process the personal data of EU citizens or residents, or you offer goods or services to such people, then the DPR applies to you even if you're not in the EU.").

178. General Data Protection Regulation, *supra* note 169, at 82–83 (providing conditions for imposing fines and penalties); *see also What Is GDPR?*, *supra* note 172 (providing an overview of the scope of and penalties imposed by the DPR).

179. *Id.*; *see also* General Data Protection Regulation, *supra* note 169, at 81–82.

180. *Compare* General Data Protection Regulation, *supra* note 169, at 81 ("Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered"), *with* 45 C.F.R. § 160.103 (illustrating that the United States lacks the same level of statutory protection that the European Union provides for those data subjects who believe their data has been misused or transferred for unapproved purposes); *but see* Matthias Artzt, *Territorial Scope of the GDPR from a US Perspective*, IAPP (June 26, 2018), https://iapp.org/news/a/territorial-scope-of-the-gdpr-from-a-us-perspective/ (providing examples of circumstances under which "U.S.-based enterprises may be caught by the GDPR, even though at first glance there seems to be no connection to the EU").

the data subject.[181] To this end, polling shows that many people do not fully understand the GDPR, or that many misunderstand it.[182] As such, the requirement of affirmatively asserting rights, coupled with the fact that many misunderstand the law, means that the overall effectiveness of the law may not be as extensive as it could be.

4. California Consumer Privacy Act and California Privacy Rights Act

California's privacy laws are the most stringent in the United States.[183] In 2018, The California Legislature passed the California Consumer Privacy Act (CCPA), which covers the rights of consumers whose data are collected by businesses.[184] The CCPA requires businesses to "implement and maintain reasonable security procedures and practices . . . to protect . . . personal information."[185] The CCPA grants the right to individuals in California to demand that companies disclose the personal data the company has collected on the individual.[186] Further, under the CCPA, a company that has acquired consumer data when so requested by the consumer is barred from selling customer information if the customer directs the company not to sell his or her data.[187]

181. *Everything You Need to Know About the "Right to Be Forgotten,"* GDRP.EU, https://gdpr.eu/right-to-be-forgotten/ (last visited Sept. 6, 2021).

182. *Do Consumers Know Their GDPR Data Privacy Rights?*, GDRP.EU, https://gdpr.eu/consumers-gdpr-data-privacy-rights/ (last visited Sept. 6, 2021) (listing multiple, albeit non-scientific, Twitter polls conducted by GDPR.EU to gauge individual knowledge regarding data rights).

183. Rodika Tollefson, *Which States Have the Toughest Privacy Laws?*, INFOSEC (May 20, 2019), https://resources.infosecinstitute.com/topic/which-states-have-toughest-privacy-laws/.

184. CAL. CIV. CODE § 1798.150(a)(1) (Deering 2021).

185. *Id.*

186. Kari Paul, *California's Groundbreaking Privacy Law Takes Effect in January. What Does It Do?*, GUARDIAN (Dec. 30, 2019, 3:00 AM), https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do.

187. *Id.*

The CCPA is similar to, but significantly narrower than, the GDPR.[188] Where the GDPR covers all businesses that handle user data, the CCPA protects only California residents and only applies to for-profit businesses.[189] If a customer makes a data request under the CCPA, that customer is limited to two requests per year, and the company providing the information must only provide the most recent twelve months of data.[190] Moreover, companies that comply with other laws, such as HIPAA, are exempt from the CCPA.[191] Most troubling are the penalties imposed on companies that violate the CCPA. The maximum recovery per consumer per incident is capped at $750,[192] and a maximum fine is $7500 for a business that intentionally violate the law.[193] The CCPA is a move in the right direction, but it significantly limits a customer's recovery for incidents involving his or her data. Moreover, the maximum penalty for a company is insignificant, which does little to incentivize a company to comply with the requirements of the law if the burden on the company for compliance outweighs the penalties it pays for violations of noncompliance.

The California Privacy Rights Act (CPRA) was adopted in November 2020 after a majority of California residents voted "yes" on the ballot proposition.[194] The law expands upon the CCPA, and will go into effect on January 1, 2023, superseding

188. *Id.* For instance, GDPR "affect[s] all businesses that handle user data, whereas the CCPA applies only to businesses with a gross revenue over $25m, more than 50,000 customers, or whose revenue is 50% or more based on user data." Paul, *supra* note 186.

189. Rita Heimes & Sam Pfeifle, *New California Privacy Law to Affect More than Half a Million US Companies*, IAPP (July 2, 2018), https://iapp.org/news/a/new-california-privacy-law-to-affect-more-than-half-a-million-us-companies/. The law notably excludes universities, which conduct vast amounts of research; *see id; see also* CAL CIV. CODE § 1798.140 (Deering 2021).

190. Paul, *supra* note 186.

191. CAL. CIV. CODE § 1798.145(c)(1)(A) (Deering 2021).

192. *Id.* § 1798.150(a)(1)(A).

193. *Id.* § 1798.155(b).

194. *California Proposition 24, Consumer Personal Information Law and Agency Initiative (2020)*, BALLOTPEDIA, https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020) [hereinafter, *California Proposition 24*] (last visited Sept. 6,, 2021).

the CCPA.[195] The CPRA closes loopholes from the CCPA.[196] The most significant loophole in the CCPA is that it only applies to the sale of data and thus allows for large companies, like Google and Facebook, to bypass the law "by claiming [that] they [are] not selling information, [but] merely sharing it."[197] The CRPA will place numerous requirements on companies, including: companies must "not share a customer's personal information upon that customer's request;" companies must "provide customers with an opt-out option for having their . . . personal information . . . used or disclosed for advertising or marketing [purposes];" companies must obtain permission before collecting information on individuals under the age of sixteen; and companies must "correct a customer's inaccurate personal information upon [request]."[198]

The CRPA is the strongest privacy law in the United States, and it is more closely aligned with the GDPR than the CCPA.[199] While the CCPA authorizes "businesses to fix violations before being penalized," the CRPA removes this protection.[200] The CRPA also triples the maximum penalty for violations concerning minors and "authorizes civil penalties for theft of customer login information."[201] The CRPA is the trailblazer privacy law in the United States, and it "is likely to serve as the [new] standard for companies across the nation."[202]

195. Chris Micheli, *When Do Prop. 24's Privacy Protections Take Effect?*, CAL. GLOBE (Nov. 6, 2020, 2:50 PM), https://californiaglobe.com/section-2/when-do-prop-24s-privacy-protections-take-effect/.

196. *See California Proposition 24*, *supra* note 194.

197. *Id.*

198. *Id.*

199. Sam Dean, *California Voters Approve Prop. 24, Ushering in New Rules for Online Privacy*, L.A. TIMES (Nov. 4, 2020, 10:43 AM), https://www.latimes.com/business/story/2020-11-03/2020-california-election-tracking-prop-24.

200. *California Proposition 24*, *supra* note 194.

201. *Id.*

202. Dean, *supra* note 199.

B. *Laws Surrounding Unauthorized Data Use*

1. Genetic Information and Nondiscrimination Act

The Genetic Information Nondiscrimination Act (GINA)[203] is a federal law that regulates employers' and health insurance providers' use of genetic information and prohibits discrimination by those entities on the basis of a person's genetic profile.[204] GINA was enacted, in part, as a Congressional response to draconian state laws that allowed for sterilization of a person who was presumed to have genetic "defects" like mental illness, blindness, and epilepsy, among other conditions.[205] Congress was particularly concerned with the "patchwork" of state and federal laws surrounding genetic discrimination and enacted GINA to "establish[] a national and uniform basic standard . . . to fully protect the public from [genetic] discrimination."[206]

Title I of GINA prohibits discrimination by health insurers on the basis of genetic information, and Title II prohibits discrimination by employers on the basis of genetic information.[207] Similar to HIPAA, GINA defines genetic information as information from genetic tests of an individual, or from an individual's family members, or "the manifestation

203. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of 26, 29, and 42 U.S.C.).

204. *Id.* at 881–82. CONSUMER REPORTS, DIRECT-TO-CONSUMER GENETIC TESTING: THE LAW MUST PROTECT CONSUMERS' GENETIC PRIVACY 15 (2020) [hereinafter CONSUMER REPORTS]; Contreras, *supra* note 89, at 41.

205. § 2, 122 Stat. at 882 (congressional findings).

206. *Id.* at 882–83. GINA reads as follows:

> Congress has collected substantial evidence that the American public and the medical community find the existing patchwork of State and Federal laws to be confusing and inadequate to protect them from discrimination. Therefore Federal legislation establishing a national and uniform basic standard is necessary to fully protect the public from discrimination and allay their concerns about the potential for discrimination, thereby allowing individuals to take advantage of genetic testing, technologies, research, and new therapies.

Id.

207. *Id.* at 881.

of a disease or disorder in family members of [the] individual."[208] GINA further defines "genetic test" as "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites that detects genotypes, mutations, or chromosomal changes." [209] DTC genetic testing companies are not specifically referenced in GINA, but a genetic test from one of these companies would meet the broad definition of genetic test defined in the statute.[210] To that end, the results of those tests are considered genetic information.[211]

Generally, under GINA, it is unlawful for an employer to request, require, or purchase genetic information with respect to an employee or his or her family member.[212] It is also unlawful for an employer to refuse to hire, discharge, or discriminate against an employee on the basis of genetic information.[213] In the health insurance context, the Affordable Care Act (ACA) works similarly to GINA as, under the ACA, no insurance plan can reject, charge more, or refuse to pay for essential health benefits based on a pre-existing condition a person had prior to applying for coverage.[214] GINA places a strong emphasis on privacy protections.[215] The ACA's focus is enhanced consumer protections in the private health insurance market.[216] The ACA "does not specifically amend GINA," nor

208. *Id.* at 885.

209. *Id.*

210. *See, e.g.*, Lowe v. Atlas Logistics Grp. Retail Servs., LLC, 102 F. Supp. 3d 1360, 1361, 1368 (N.D. Ga. 2015) (holding that Congress struck a broad definition of "genetic tests" and that an employer violated GINA when it conducted genetic testing on employees via cheek swab to identify the culprit of defecation episodes in the employer's warehouse).

211. CONSUMER REPORTS, *supra* note 204, at 15.

212. § 202, 122 Stat. at 907.

213. *Id.*

214. *Coverage for Pre-Existing Conditions*, HEALTHCARE.GOV, https://www.healthcare.gov/coverage/pre-existing-conditions/ (last visited Aug. 28, 2021).

215. AMANDA K. SARATA, JAMES V. DEBERGH & JENNIFER STAMAN, CONG. RSCH. SERV., THE GENETIC INFORMATION NONDISCRIMINATION ACT OF 2008 AND THE PATIENT PROTECTION AND AFFORDABLE CARE ACT OF 2010: OVERVIEW AND LEGAL ANALYSIS OF POTENTIAL INTERACTIONS 11 (2011), https://www.genome.gov/Pages/PolicyEthics/GeneticDiscrimination/CRS_GINA_and_ACA.pdf.

216. *Id.*

does it reference GINA.[217] In effect, the ACA fills many of the gaps in protection left by GINA.[218]

"Unlike the informed consent requirements under the Common Rule and HIPAA, GINA does not require that a user of individual genetic data explain the proposed use and seek the individual's consent to that use."[219] Rather, GINA prohibits listed categories of conduct mentioned above and provides a legal remedy for conduct that violates the statute.[220] Since 2010, the Equal Employment Opportunity Commission (EEOC) has tallied at least two hundred charges per year under GINA.[221] The most significant penalty under GINA was a jury verdict in a case brought by two employees against their employer, Atlas Logistics.[222] Within Atlas's storage warehouses, an unknown employee began "habitually defecating."[223] Atlas then requested cheek swab DNA samples from two employees to compare with the DNA from the fecal matter.[224] Neither of the two employees were matches, and they thereafter filed an action under GINA.[225] A jury awarded the workers a $2.2 million verdict for being required to submit DNA samples in violation of GINA.[226]

217. *Id.*

218. *See* Michelle Andrews, *Has Genetic Privacy Been Strained by Trump's Recent ACA Moves?*, NPR (July 11, 2018, 8:02 AM), https://www.npr.org/sections/health-shots/2018/07/11/627287642/has-genetic-privacy-been-strained-by-trumps-recent-aca-moves.

219. Contreras, *supra* note 89, at 42.

220. *Id.*; *See also* Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-223, §§ 202, 207, 122 Stat. 907, 914–15.

221. *Genetic Information Non-Discrimination Act Charges (Charges filed with EEOC) (Includes Concurrent Charges with Title VII, ADEA, ADA, and EPA) FY 2010-2020*, EEOC, https://www.eeoc.gov/eeoc/statistics/enforcement/genetic.cfm (last visited Aug. 28, 2021).

222. Gina Kolata, *Georgia: $2.2 Million Penalty for Illegal DNA Testing*, N.Y. TIMES (June 22, 2015), https://www.nytimes.com/2015/06/23/us/georgia-dollar2-2-million-penalty-for-illegal-dna-testing.html?_r_0.

223. *See* Lowe v. Atlas Logistics Grp. Retail Servs., 102 F. Supp. 3d 1360, 1361 (N.D. Ga. 2015).

224. *Id.*

225. *Id.*

226. Kolata, *supra* note 222.

GINA provides relief to individuals when an employer or health insurance provider uses genetic tests or other genetic information in discriminatory or prohibited ways under the statute, but "GINA does not apply to life insurance, disability insurance, long-term care insurance, or other potential discriminatory uses of genetic information."[227] Moreover, GINA does not specifically reference DTC genetic testing companies as it relates to sharing information with many categories of third parties outside the context of discrimination.[228] Nonetheless, GINA is a concrete example of the prohibition on the use of genetic information, and it is possible that it could be expanded to cover genetic information uses in other contexts, like when pharmaceutical companies use genetic information from 23andMe for research purposes.

2. The Americans with Disabilities Act

The Americans with Disabilities Act (ADA) prohibits discrimination based on disability in employment and public accommodations.[229] Public accommodations include most places people may go in public and effectively hinges on whether the operations of an entity affect commerce.[230] The ADA defines disability as a physical or mental impairment that substantially limits at least one major life activity of the individual.[231] Disability also means having a record of such impairment, or being regarded as having such impairment.[232] Major life activities are those which include sitting, walking, sleeping, breathing, and concentrating, among most other activities a human performs.[233] Major bodily functions are also

227. Mark A. Rothstein, *GINA, the ADA, and Genetic Discrimination in Employment*, 36 J.L. MED. & ETHICS 837, 837–38 (2008) (discussing the deficiencies of GINA's reach, as well as pro-employer loopholes for genetic testing related to the ADA).

228. CONSUMER REPORTS, *supra* note 204, at 15.

229. *See* 42 U.S.C. § 12112, 12182.

230. § 12181(7).

231. § 12102(1).

232. *Id.*

233. § 12102(2)(A)(listing all major life activities for the purposes of the ADA).

major life activities, including immune, respiratory, neurological, and endocrine function, among other functions of the body's major systems.[234] If a disability "substantially limits" an individual, then the individual falls under the protection of the ADA.

An individual with a genetic trait that limits a major life activity is protected by the ADA if that trait has manifested itself.[235] However, it is less clear if the ADA would protect an individual where a genetic trait only *may* increase the probability that the individual will experience a substantial impairment in the future.[236] The ADA does not cover discrimination based on a genetic trait where the individual with that trait is predisposed to a manifestation but is at that time asymptomatic.[237] An employer, therefore, who acquires genetic information on an individual, where the individual is predisposed due to a genetic trait but is currently asymptomatic, faces no liability under the ADA if the employer discriminates based on this genetic information. If an asymptomatic individual like the one described takes a genetic test from a business like 23andMe, this could prove harmful for the individual down the line if the genetic information was leaked in a breach. Because laws like the ADA are lacking in protecting certain individuals, other laws must be implemented to decrease the possibility that an employer would ever attain such genetic information in the first place.

IV. FAULT-BASED TORTS ARE A SUBOPTIMAL SOLUTION

As evidenced by the survey of current laws discussed *supra*, there is a need to pass additional laws to protect genetic data and the people to whom it pertains. This Part details why fault-

234. § 12102(2)(B) (listing all major bodily functions for the purposes of the ADA).

235. *See* §12102.

236. *See* Field et al., *supra* note 133, at 25.

237. Carly B. Eisenberg, Note, *Genetic Predispositions v. Present Disabilities: Why Genetically Predisposed Asymptomatic Individuals Are Not Protected by the Amended ADA*, 15 B.U. J. SCI. & TECH. L. 130, 149–50 (2010).

based torts are not the best solution to protect consumers in the context of genetic data sharing.

A. *Hypothetical on the Possible Effects of Genetic Data Involved in a Breach*

The following is a hypothetical of what could happen to a DTC genetic testing company customer if the customer's genetic information gets disclosed due to a security breach.

Alex received a genetic testing kit for her birthday and found out she has an increased risk of diabetes and certain types of cancer. Down the line, Alex begins receiving targeted advertisements for diabetes and cancer treatment and prevention options. She never could have imagined that taking an at-home genetic test could lead to pervasive advertising regarding her private medical information. Alex, like most people, is not trained to understand long and complicated terms of service and privacy agreements that she supposedly consented to when she took the genetic test.[238] Alex lost the autonomy to choose to not have pervasive advertising regarding her sensitive genetic information plastered all over the webpages she visits. If that company valued transparency, it would not bury its data sharing policies in lengthy legal documents that people often fail to read.[239] Targeted ads may be the least of Alex's worries when it comes to genetic information. If banks or insurers, among others, get this information, the consequences could be abysmal.[240] Such a hypothetical is more likely to happen now and in the future because of the growing

238. One study that analyzed 500 term contracts found that 498 of the contracts required an average of more than fourteen years of education to understand. Dustin Patar, *Most Online 'Terms of Service' Are Incomprehensible to Adults, Study Finds*, VICE (Feb. 12, 2019, 2:51 PM), https://www.vice.com/en/article/xwbg7j/online-contract-terms-of-service-are-incomprehensible-to-adults-study-finds.

239. *See, e.g.*, *Privacy Statement*, *supra* note 10 (showing that part of 23andMe's data sharing policy is buried within a lengthy legal document).

240. *See, e.g.*, MEDLINEPLUS, HELP ME UNDERSTAND GENETICS 173 (2020), https://medlineplus.gov/download/genetics/understanding/primer.pdf ("The results of genetic testing may impact your ability to obtain life, disability, or long-term care insurance.").

ease of re-identifying de-identified data, meaning Alex's genetic data not only could be acquired by bad actors, but also that those actors could then trace that data back to Alex.

Some laws, like GINA, could protect a person in the above situation as it relates to health insurance or employment,[241] but that would only penalize the end user, *i.e.*, the employer or health insurer for obtaining and using that information. Under most laws, however, it would be difficult to penalize the company that was supposed to safely store her genetic information without proving negligence on part of the company, and it would also be difficult under most fault-based theories for Alex to receive compensation for the exposure of her immutable information without proving the company breached its standard of care.[242]

B. *Negligent or Intentional Conduct-Based Torts Are Not Optimal*

There are various tort claims available to victims of genetic privacy violations.[243] Two prominent theories of recovery in the genetic data context are infliction of emotional distress and breach of fiduciary duty.[244] In theory, these types of tort claims could be successful but, in reality, the barriers brought on by fault-based tort law prevents victims of genetic data breaches from succeeding on such claims.[245]

1. Emotional distress resulting from genetic data disclosure

The *Restatement (Third) of Torts* states that "[a]n actor whose negligent conduct causes serious emotional harm to another is subject to liability to the other if the conduct . . . occurs in the

241. *See* discussion *supra* Section III.B.

242. *See* Ifeoma Ajunwa, *Genetic Testing Meets Big Data: Tort and Contract Law Issues*, 75 OHIO ST. L.J. 1225, 1253–55 (2014); *see also* Benjamin Sundholm, *Strict Liability for Genetic Privacy Violations in the Age of Big Data*, 49 UNIV. MEM. L. REV. 759, 790 (2019).

243. *See, e.g.*, Ajunwa, *supra* note 242, at 1248–52 (providing examples of the possible tort claims, including negligent infliction of emotional distress and breach of fiduciary duty, that a victim of a genetic privacy violation may be able to raise).

244. *See id.*

245. *See id.* at 1253–55.

course of specified categories of activities, undertakings, or relationships in which negligent conduct is especially likely to cause serious emotional harm."[246] Genetic information misuse can cause serious emotional injury and diminished autonomy, which can then lead to lasting traumatic effects.[247] However, it is difficult for plaintiffs to successfully pursue remedies for emotional harms.[248] For example, in one case involving a divorce between a plaintiff and his wife, a hospital turned over the plaintiff's medical records to the wife's attorney. These records documented plaintiff's past psychological and psychiatric care but were determined to be outside the scope of the court order.[249] When the attorney refused to return those records, the plaintiff countersued the hospital for intentional and negligent infliction of emotional distress.[250] Intentional infliction of emotional distress requires extreme and outrageous conduct, which the court determined was absent on part of the hospital because it could have reasonably interpreted that information to be within the scope of the court order.[251] The hospital also was not liable under negligent infliction of emotional distress because the court held there was insufficient evidence to conclude the hospital should have known disclosing the records would cause plaintiff emotional distress.[252] Thus, the plaintiff did not succeed on either claim.[253]

If the above example were to take place within the context of genetic testing, it would be very difficult to prove that a DTC

246. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 47 (A.L.I. 2012).

247. *See* Zhansheng Chen, Kipling D. Williams, Julie Fitness & Nicola C. Newton, *When Hurt Will Not Heal: Exploring the Capacity to Relive Social and Physical Pain*, 19 PSYCH. SCI. 789, 793–94 (2008), https://journals.sagepub.com/doi/pdf/10.1111/j.1467-9280.2008.02158.x ("[R]eliving social pain triggers higher levels of pain than reliving physical pain."); *see also* M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1144–47 (2011) (describing the causes and effects of subjectively-felt privacy harms).

248. *See* Ajunwa, *supra* note 242, at 1254–55.

249. St. Anthony's Med. Ctr. v. H.S.H., 974 S.W.2d 606, 608 (Mo. Ct. App. 1998).

250. *Id.* at 608–09.

251. *Id.* at 611.

252. *Id.* at 613.

253. *Id.*

genetic testing company acted in an extreme or outrageous manner in the event of a security breach. These companies have cyber protections in place,[254] but few laws specify the level of security they need to maintain.[255]

This theory does not regulate a company's cybersecurity practices, and it would be difficult for a plaintiff to succeed on intentional or negligent infliction of emotional distress claims.[256] Therefore, these claims do nothing to deter subpar cybersecurity practices, and do little to protect customers' interests.

2. Violations of fiduciary duties resulting from genetic data disclosures

One author notes that a breach of fiduciary duty claim would be a customer's strongest tort claim in the genetic testing context.[257] For a breach of fiduciary duty claim to prevail, the plaintiff must first show the existence of a fiduciary relationship between parties.[258] A fiduciary relationship is "one in which special confidence and trust is reposed in the integrity and fidelity of another and there is a resulting position of superiority or influence, acquired by virtue of this special trust."[259] Fiduciary relationships are imposed where one party to a relationship can exert influence or dominance over the

254. For instance, 23andMe uses "[a]n automated internal assessment that reveals vulnerabilities by comparing the organization's [security structure] with best practices, i.e., contrasting existing practices against well-accepted standards." Bob Barker, *Which Approach to Cyber Risk Oversight is Best – Google, or 23andMe?*, CYBERNANCE: CYBERGOVERNANCE J. (May 16, 2016), https://www.cybernance.com/approach-cyber-risk-oversight-best-google-23andme/.

255. *See* Catherine Roberts, *Your Genetic Data Isn't Safe*, CONSUMER REPS., (July 23, 2020), https://www.consumerreports.org/health-privacy/your-genetic-data-isnt-safe-direct-to-consumer-genetic-testing-a1009742549/.

256. *See* Ajunwa, *supra* note 242, at 1254 (providing that a DTC genetic testing company could argue that such attacks are unforeseeable and that it would be unreasonable to hold the company liable for the actions of hackers). Moreover, establishing damages for plaintiffs "represents another stumbling point" because such damages are non-pecuniary in nature. *Id.*

257. *Id.* at 1249.

258. *Id.* at 1250 (citing Tornado Techs., Inc. v. Quality Control Inspection, Inc., 977 N.E.2d 122, 127 (Ohio Ct. App. 2012)).

259. In re Termination of Emp. of Pratt, 321 N.E.2d 603, 609 (Ohio 1974).

other party,[260] including relationships between: an attorney and his client, a principal and her agent, a guardian and his ward, and a doctor and her patient.[261] Fiduciary law is able to "redress situations where 'the ordinary laws of contract, tort, and unjust enrichment are silent or insufficient.'"[262]

It is conceivable that the relationship between DTC genetic testing companies and their customers could be a fiduciary relationship because one could argue this is a relationship of "special trust" regarding health information, not unlike a doctor-patient relationship.[263] But, as with emotional distress claims, it would be difficult for a plaintiff to prevail on a breach of fiduciary duty claim in the genetic data context.[264] For instance, as one court concluded, fiduciary duties do not exist unless the defendant expressly recognized and accepted the duties the plaintiffs allege.[265]

DTC genetic testing companies often include in their terms of service or privacy policy an express authorization for that company to sell or transfer customers' genetic data.[266] With customers signing off on DTC genetic testing company terms of service and privacy policies, it is unlikely a plaintiff customer could successfully argue that a company recognized and accepted fiduciary duties to customers.[267] Moreover, the typical fiduciary relationship at least partially occurs face-to-face, like

260. *Fiduciary Duty*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/fiduciary_duty (last visited Aug. 19, 2021).

261. *Id.*

262. Ajunwa, *supra* note 242, at 1250 (quoting Thomas L. Hafemeister & Joshua Hinckley Porter, *Don't Let Go of the Rope: Reducing Readmissions by Recognizing Hospitals' Fiduciary Duties to Their Discharged Patients*, 62 AM. UNIV. L. REV. 513, 544 (2013)).

263. *See* Sundholm, *supra* note 242, at 787.

264. *See supra* Section IV.B.1.

265. Greenberg v. Mia. Child.'s Hosp. Rsch. Inst., Inc., 264 F. Supp. 2d 1064, 1071–72 (S.D. Fla. 2003).

266. *See supra* text accompanying notes 35–36; *see, e.g.*, *Privacy Highlights*, *supra* note 71 ("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.").

267. *See Greenberg*, 264 F. Supp. 2d at 1071–72.

with doctor-patient relationships.[268] On the other hand, the relationship between genetic testing companies and their customers occurs over the Internet with little interaction, making it unlikely that courts would find such an attenuated interaction between a genetic testing company and its customer to amount to a fiduciary relationship.[269] No special relationship has occurred like that in a doctor-patient or lawyer-client relationship, meaning fiduciary duties likely do not exist in the genetic testing context.[270]

Fiduciary duty breaches can occur through negligent or intentional conduct.[271] Even if courts recognized a fiduciary relationship, in the event of a data breach, a customer plaintiff would find it difficult to establish fault, intentional or negligent, on part of the company when that company has satisfactory data security to guard against hackers.[272] Therefore, breach of fiduciary duty is not a viable claim for a DTC genetic testing customer because a fiduciary relationship likely does not exist, and even if it did, the company would be unlikely to have breached its duty in the event of a data breach.

V. THE NEED FOR CHANGE: DETER AND COMPENSATE

This Part proposes a solution in two forms. Section A details the first main goal of this proposed law—to protect customers to the greatest extent possible. Section B details the second main goal of this proposed law—to regulate the data sharing activity of DTC genetic testing companies.

268. *See* Ajunwa, *supra* note 242, at 1251.

269. *Id.* at 1251–52.

270. *See id.*

271. *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 49 cmt. c, d (A.L.I. 2000); *see also* Roy Simon, *Legal Malpractice and Breach of Fiduciary Duty—Part I*, N.Y. LEGAL ETHICS REP. (Apr. 2006), http://www.newyorklegalethics.com/legal-malpractice-breach-of-fiduciary-duty-part-i/ (explaining that a lawyer can unintentionally, *i.e.*, negligently, or intentionally breach his or her fiduciary duty to a client).

272. *See Security Breach – How Businesses May Be Liable*, HG.ORG https://www.hg.org/legal-articles/security-breach-how-businesses-may-be-liable-44358 (last visited Aug. 29, 2021, 11:19 AM).

The DTC genetic testing market is an imperfect system at best. Millions of people hand over precious and immutable information to these companies for safe keeping.[273] When a customer contributes his or her DNA to one of these companies, it implicates that customer's relatives as well.[274] Most of all, these companies reap the benefits of customer samples but are immune from most liability.[275]

A federal statute is one option to uniformly regulate this largely unregulated industry. One federal statute would be preferable to multiple state laws because it would achieve uniform compliance on the part of the companies, rather than a company being required to comply with differing standards across states. This statute would seek to resolve the most pressing problems with the DTC genetic testing industry in practical ways. The first major goal of this statute would be to recognize and compensate individuals whose data is involved in a data breach by holding genetic testing companies accountable for such breaches, regardless of fault.

A. *Solution I: Strict Liability*

Strict liability and negligence are theories that courts apply in tort liability cases and are implicated in damage awards.[276] To compare these two theories based on economic efficiency, there must be a distinction between unilateral and bilateral accidents.[277] Unilateral accidents are those in which only the injury-causing party can affect the probability of accident occurrence and the magnitude of loss due to an accident.[278] In

273. Regalado, *supra* note 7.

274. *See* Julia Belluz, *Genetic Testing Brings Families Together*, VOX (Dec. 18, 2014, 2:07 PM), https://www.vox.com/2014/9/9/6107039/23andme-ancestry-dna-testing.

275. *See supra* Section I.A (discussing the value of DTC genetic libraries); *supra* Section II.A (describing how these companies often fall outside the scope of federal regulation).

276. Vaia Karapanou, *Strict Liability Versus Negligence*, ENCYC. L. & ECON. (Dec. 1, 2014), https://link.springer.com/referenceworkentry/10.1007%2F978-1-4614-7883-6_528-1.

277. *Id.*

278. *Id.*

bilateral accidents, both parties affect probability of occurrence and magnitude of loss.[279] Data breaches involving genetic testing companies fall under the column of unilateral accidents, because only the injury-causing party—the company—can affect the probability of occurrence and magnitude of the breach.[280] Customers have no ability to affect breach probability or magnitude because they have no control over a company's security.

Where, as here, damages are compensatory and the level of care, i.e., security, is set equal to its optimal level, strict liability induces optimal precaution on part of the genetic testing company and induces the company to engage in optimal levels of activity, where activity is defined as data sharing or other acts making a breach more likely to occur.[281] Negligence, on the other hand, does not incentivize a company to maintain optimal activity levels because as long as the company abides by a law's standards for data security, the company will not be liable in the event of a breach.[282] This leaves customers with no recognition and no compensation when their immutable data is taken in a breach with the potential to be used for nefarious purposes. Negligence, therefore, goes against a goal of this law to recognize and compensate individuals. As a result, strict liability is a better option to protect customers and put the onus on the company to decide optimal activity levels of data sharing, or else face liability in the form of compensatory damages that outweigh profits gained by additional, unnecessary data sharing. As one author notes, if defendants

279. *Id.*

280. *See id.*

281. *Id.*; *see also Economic Analysis of Alternative Standards of Liability in Accident Law*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y. AT HARV. UNIV.: THE BRIDGE, https://cyber.harvard.edu/bridge/LawEconomics/neg-liab.htm (last visited Nov. 10, 2021) [hereinafter *Standards of Liability*].

282. *See Standards of Liability*, *supra* note 281.

are in the best position to adjust the levels of their activities, a strict liability rule is preferred.[283]

To illustrate the above concepts in a more common context, consider the following example. Suppose these concepts are taken in the context of roadway accidents, where a car driver is equal to a genetic testing customer; a truck driver is equal to the genetic testing company; and a collision is equal to a data breach. Under a strict liability theory, a truck driver (company) is induced to take optimal precautions and will be discouraged from excessive activity levels of driving (data sharing).[284] This is because in this example a truck driver (company) would be liable for any collisions (breaches) that occur.[285] By being forced to pay for any collision (breach), the truck driver (company) will decline to take trips (share data) whenever the resultant savings, in terms of decreased liability, outweigh the potential profit.[286] Under a negligence theory on the other hand, truck drivers (companies) will be incentivized to maintain high activity driving (data sharing) levels because, knowing the truck driver (company) can escape liability as long as he abides by the prescribed level of care (data security laws), the truck driver (company) will continue to drive (share data) to derive marginal profits from additional trips.[287] Under a negligence theory, if a car driver (customer) is injured by a truck, but the truck driver (company) is not liable if he took the required precautions, it leaves the car driver (customer) with injuries but no compensation.[288]

This proposed federal law would provide a private right of action under a strict liability theory for a customer whose data was subject to a breach, where the remedy is compensatory damages. A strict liability theory reduces costs of litigation

283. *Id.* at 273; s*ee* Steven Shavell, *Strict Liability Versus Negligence*, 9 J. LEGAL STUD. 1, 2–3 (1980).

284. *Standards of Liability*, *supra* note 281.

285. *Id.*

286. *Id.*

287. *Id.*

288. *Id.*

compared to a negligence theory because courts do not need to determine the level of care the defendant is held to, nor whether the defendant has met that level of care.[289] Further, strict liability can be described as an "insurance function," which permits companies to spread risk to all customers who purchase testing kits.[290] For instance, if one in one thousand customers are harmed from a breach, strict liability will impose on every customer 1/1000 of the cost of the harm in the form of slightly higher prices for testing kits, rather than having the harmed customer bear the whole burden if she cannot prove the company was negligent.[291] A strict liability theory could incentivize companies to use this insurance function to more accurately reflect the costs of the services and associated harm, which will result in a pattern of product prices to guide potential "customers to select safer companies and avoid more dangerous ones." [292]

The inevitable barrier for customer plaintiffs to overcome in the event they bring suit will be proving harm. Regardless of the theory of fault, the plaintiff must show the harm derived from her genetic data, and that the genetic data was taken from the genetic testing company when it was breached.[293] In other words, the plaintiff still must prove the company caused the harm in some way.[294] It may also be difficult to determine if one's genetic data was taken from the genetic testing company, or from a third party with whom the genetic data was shared.[295] However, as the previous example demonstrates, strict liability

289. *See id.* (noting, however, that reduced costs of strict liability litigation may be offset by a likely increase in the overall amount of strict liability cases brought to court).

290. *Id.*

291. *Id.*

292. *See Standards of Liability*, *supra* note 281; *see also* Guido Calabresi, *Some Thoughts on Risk Distribution and the Law of Torts*, 70 YALE L. J. 499, 505 (1961).

293. *See* Sundholm, *supra* note 242, at 790.

294. *See id.*

295. Eric Ravenscraft, *How to Protect Your DNA Data Before and After Taking an at-Home Test*, N.Y. TIMES (June 12, 2019), https://www.nytimes.com/2019/06/12/smarter-living/how-to-protect-your-dna-data.html.

is still more plaintiff-friendly than negligence.[296] Strict liability theory evolved specifically for instances when a plaintiff could not feasibly prove negligence.[297] One author provides an example of computer software: if a product is overly complex, it may be nearly impossible for a customer who knows little about the workings of the product to identify the source of the negligence which was responsible for the specific defect.[298] The same applies for genetic data breaches. It is unlikely a plaintiff would know enough about the workings of a company's complex security systems to identify the defective aspects that led to a breach. But under strict liability, a plaintiff only must show that it was in fact defective,[299] which can be shown by circumstantial evidence. For instance, a customer only had her genetic data stored with one company, she experienced harm that derived from someone's knowledge of that data, and therefore the company's security must have been defective.

Therefore, though still difficult for a plaintiff to prevail, a strict liability theory of fault under the federal law would provide customers with the best opportunity to be recognized and compensated when their genetic data is involved in a breach and used to harm them. The strict liability theory will also serve to deter companies from excessive data sharing and will hold companies accountable for proven harms.

B. *Solution II: Federal Oversight and Regulation*

The second major goal of this new federal statute would be to oversee and regulate DTC genetic testing companies. This is accomplished by incentivizing security and fining and censuring companies that get breached.

The law will designate the Federal Trade Commission (FTC) as the primary agency that oversees and regulates this industry.

296. *See Standards of Liability*, *supra* note 281.

297. L. Nancy Birnbaum, *Strict Products Liability and Computer Software,* 8 J. MARSHALL J. INFO. TECH. & PRIV. L. 135, 142 (1988).

298. *Id.*

299. *Id.*

Though it would likely require increased funding, the FTC is the best suited agency for the task because of its "dual mission to protect consumers and promote competition" in industry.[300] Specifically, the FTC seeks to protect consumers by stopping unfair and deceptive practices in the marketplace, conducting investigations, suing companies that violate the law, and educating consumers and companies about their rights and responsibilities.[301] Moreover, the FTC has "brought dozens of cases challenging deceptive or unfair practices related to consumer privacy and data security—including a settlement with a business that sold products based on at-home genetic testing, but allegedly failed to provide reasonable security for consumers' personal information."[302]

First, the law must incentivize security. This incentive program would come in the form of tax deductions for companies that meet certain data security standards. A tax deduction lowers a company's tax liability by lowering its taxable income.[303] Typically, deductions are expenses that the company incurs during a given year that can be subtracted from that company's otherwise taxable income.[304] Here, this law would allow genetic testing companies to lower their taxable income by deducting the cost of data privacy and security

300. *What We Do*, F.T.C., https://www.ftc.gov/about-ftc/what-we-do (last visited Nov. 10, 2021); *see also* Chelsea Weiermiller, Note, *The Future of Direct-to-Consumer Genetic Testing: Regulation and Innovation*, 16 N.C. J.L. & TECH. 137, 158–59 (2015), https://scholarship.law.unc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1290&context=ncjolt (arguing that the FTC is in the best position to regulate DTC genetic testing companies).

301. *What We Do*, *supra* note 300; *see also* Matthew Piehl, *Regulating Hype and Hope: A Business Ethics Model Approach to Potential Oversight of Direct-to-Consumer Genetic Tests*, 16 MICH. STATE UNIV. J. MED. & L. 59, 76–77 (2011) ("The FTC administers many consumer protection laws, especially those related to unfair or deceptive trade practices, such as misleading advertising claims. . . . [H]owever, the FTC has not yet taken action against DTC genetic companies.").

302. Lesley Fair, *DNA Test Kits: Consider the Privacy Implications*, F.T.C.: CONSUMER INFO. BLOG (Dec. 12, 2017), https://www.consumer.ftc.gov/blog/2017/12/dna-test-kits-consider-privacy-implications.

303. Julia Kagan, *Tax Deduction*, INVESTOPEDIA, https://www.investopedia.com/terms/t/tax-deduction.asp (Oct. 5, 2021).

304. *Id.*

expenses, but such deductions will require a limit so companies cannot game the system, similar to how certain corporate deduction limits work.[305] Other areas of industry employ similar tax deduction programs, for example, the pharmaceutical industry. Pharmaceutical companies can deduct the cost of advertising expenses from federal taxes.[306] While many are pushing for a repeal of the pharmaceutical tax deductions for advertising,[307] the deductions for genetic testing companies would serve to protect consumers, unlike the pharmaceutical deductions that increase aggressive targeted drug advertisements to consumers.[308]

The tax deduction program would also serve as an incentive program. This program would be based on a rating scale, similar to how the S&P Global ratings scale grades the creditworthiness of bonds to inform investors.[309] The rating scale would be set against varying levels of government-determined data privacy and security standards, where a company that spends more and meets the highest standards receives a larger tax deduction, and where a company that maintains minimal security below a specified grade receives a smaller deduction or no deduction at all. Moreover, the

305. *See, e.g.*, I.R.S., DEP'T OF THE TREASURY, PUB. NO. 542, CORPORATIONS 11 (2019) (explaining how corporations must limit their deductions on specific types of income, like dividends).

306. Elaine Silvestrini, *Big Pharma's $6 Billion Tax Deduction Under Fire*, DRUGWATCH (Apr. 3, 2018), https://www.drugwatch.com/news/2018/04/03/big-pharmas-6-billion-tax-deduction-under-fire/.

307. *See id.*; Press Release, Jeanne Shaheen, Shaheen Reintroduces Bill to Stop Big Pharma from Exploiting Advertising Tax Loophole (Jan. 20, 2021), https://www.shaheen.senate.gov/news/press/shaheen-reintroduces-bill-to-stop-big-pharma-from-exploiting-advertising-tax-loophole.

308. *See* Thomas Sullivan, *Senators Once Again Taking Up the DTC Tax Write-Off*, POL'Y & MED., https://www.policymed.com/2018/03/senators-once-again-taking-up-the-dtc-tax-write-off.html (May 4, 2018) (noting that senators do not want taxpayers subsidizing pharmaceutical ads, in part because these companies have "spent more on sales and marketing . . . than they [have] on research and development").

309. *See Intro to Credit Ratings*, S&P GLOB., https://www.spglobal.com/ratings/en/about/intro-to-credit-ratings (last visited Nov. 10, 2021) (describing the classic rating scale, which ranges from AAA as the highest rating, to D as the lowest rating).

company's rating would be required under the law to be posted conspicuously on the homepage of each company's website, similar to restrictive legends noted on restricted stocks and securities.[310] This system, like a credit rating system, would inform customers of the potential risk they would be taking on by providing a given company with their genetic information. This would incentivize companies to prioritize their security systems, and it would also steer customers in the direction of safer companies. The FTC advises potential customers to not only look at price and performance when choosing a DTC genetic testing company, but also to scrutinize each company's security and privacy procedures as it relates to sharing personal data.[311] This new system would bolster FTC guidance by making it easier for potential customers to research a company's security and privacy procedures.

Another reason the FTC would be well suited to carry out this policy is because it promotes competition in industry.[312] With this incentive plan, one could imagine anticompetitive behavior. For instance, a smaller company that does not meet the higher quality security standards of this new law would likely have a smaller market share over time as bigger companies continue to succeed under the law. As such, those smaller companies could enter into deals with larger companies, where the smaller company gets the benefit of a large payout in the merger or acquisition, and the larger company acquires the smaller company's assets, including its genetic data.[313] In this instance, the FTC has the ability to challenge anticompetitive mergers that could harm consumers

310. *See Rule 144: Selling Restricted and Control Securities*, U.S. SEC. & EXCH. COMM'N (Jan. 16, 2013), https://www.sec.gov/reportspubs/investor-publications/investorpubsrule144htm.html [hereinafter *Rule 144*].

311. *See* Fair, *supra* note 302.

312. *See Anticompetitive Practices*, F.T.C., https://www.ftc.gov/enforcement/anticompetitive-practices (last visited Nov. 10, 2021) ("The FTC takes action to stop and prevent unfair business practices that are likely to reduce competition and lead to higher prices, reduced quality or levels of service, or less innovation.").

313. *See, e.g.*, de la Merced, *supra* note 46.

in the form of fewer choices.[314] Thus, the FTC can work to ensure that this industry is not monopolized under the new law.

Next, DTC genetic testing companies that are breached would be fined and required to publish all data breaches on their respective websites under the new law. The new law would function similar to the GDRP, where a company that experiences a data breach must report the breach to the FTC within seventy-two hours of the breach being found.[315] Also like the GDPR, genetic testing companies would be required to conduct data protection impact assessments whenever a new project, such as data sharing with a third party, is likely a high risk to customers' information.[316] The assessments are aimed to highlight risks and demonstrate compliance with the new law's standards for security and customer protection.[317] In the event of a breach, after disclosure to the FTC, the company would be required to work in conjunction with the FTC to publish details of the breach on the company's site, similar to how companies would be required to report their security rating on their respective websites.[318] Moreover, like the security rating, breach history and details must be easily accessible from the homepage of the site, such that companies cannot bury breaches.[319] This framework accomplishes two goals: first, it informs potential and existing customers of the likelihood of data breaches, and second, it incentivizes companies to invest significantly in cybersecurity to avoid the public embarrassment of publishing a long list of data breaches on its website.

The publication requirement may be a more effective tactic than only a monetary fine because a fine to a large company

314. *See Anticompetitive Practices*, *supra* note 312. The FTC enforces anticompetitive conduct through Section 5 of the Federal Trade Commission Act. *See id.*; *see also* 15 U.S.C. § 45 (2021).

315. *See What Does GDPR Stand for?*, *supra* note 174.

316. *See DPIA*, *supra* note 175.

317. *See id.*

318. *See supra* text accompanying note 310.

319. *See Rule 144*, *supra* note 310.

often is not powerful enough to change behavior,[320] but public shame can be powerful.[321] Using a shaming tool is not a form of retribution, but rather it aims to deter similar behavior in the future.[322] Since the FTC already prosecutes lax cybersecurity as a form of unfair trade practice,[323] it would be well-suited to oversee the publishing requirement. The FTC has already settled over twenty cases that it initiated on lax cybersecurity grounds,[324] meaning precedent exists on which this new law can expand.

Finally, when a genetic testing company mishandles user data, the new law would focus on imposing large fines. The FTC has already shown a willingness to impose massive fines on technology companies that allow third parties to exploit customer data.[325] The proposed law would specify guidelines

320. *See* Jason M. Breslow, *How $80 Billion in Corporate Fines Can Become $48 Billion in Tax Breaks*, PBS: FRONTLINE (Dec. 4, 2015), https://www.pbs.org/wgbh/frontline/article/how-80-billion-in-coporate-fines-can-become-48-billion-in-tax-breaks/ (noting that corporate fines often result in corporate tax breaks); *see also Are Corporate Fines High Enough to Make a Difference?*, FREAKONOMICS (July 27, 2012, 10:23 AM), https://freakonomics.com/2012/07/27/are-corporate-fines-high-enough-to-make-a-difference/ (citing a study that found that even large fines levied against companies are not high enough to change behavior).

321. One study noted that public shaming of private companies such as 23andMe created "short-term negative sentiment toward [the companies]", and that shaming of public companies created small stock dips. Joe Harpaz, *Public Shaming of Big Companies Not as Big a Deal, but Not Going Away Anytime Soon*, FORBES (June 26, 2017, 9:44 AM), https://www.forbes.com/sites/joeharpaz/2017/06/26/public-shaming-of-big-companies-not-as-big-a-deal-as-youd-think-but-not-going-away-anytime-soon/?sh=48839d016333. The goal of the law is not to bring a company to its knees for a breach, but rather to give it a push to do better. *See id.*

322. *See* Tovia Smith, *Companies 'Named and Shamed' for Bad Behavior*, NPR (Mar. 7, 2010, 12:00 AM), https://www.npr.org/templates/story/story.php?storyId=124357844 (noting that the goal of shaming is deterrence, not retribution, and that these "high-profile mea culpas" also tend to satisfy a public that is "increasingly frustrated by corporate wrongdoing").

323. Thomas Rohback & Patricia Carreiro, *How 3 Agencies Prosecute Lax Cybersecurity*, LAW360 (Mar. 2, 2016, 10:42 AM), https://www.law360.com/articles/764422/how-3-agencies-prosecute-lax-cybersecurity ("Section 5 of the FTC Act authorizes the FTC to prosecute 'unfair or deceptive acts or practices' . . . . [T]he FTC has settled over 20 cases alleging that a company's failure to reasonably safeguard consumer data is an unfair practice.").

324. *Id.*

325. The FTC handed down a nearly $5 billion fine to Facebook for mishandling user data and improperly sharing data with third parties, resulting in privacy violations. Cecilia Kang, *F.T.C. Approves Facebook Fines of About $5 Billion*, N.Y. TIMES (July 12, 2019), https://www.nytimes.com/2019/07/12/technology/facebook-ftc-fine.html. The FTC has also

that DTC genetic testing companies must follow to avoid fines, and it would provide guidance on when a fine is to be imposed, for instance, when a company violates privacy policies. These fines, unlike the shaming tool, act as retribution.[326] While fines or censure, alone, may be mild penalties to these companies,[327] the new law incorporates both deterrence and retribution to ensure genetic testing companies abide by practices that are not only developed for profit reasons, but also for customer protection.

Therefore, the new law's goal of oversight and regulation, apart from strict liability, is accomplished in three broad ways. First, the tax deduction program would incentivize companies to maintain top-level cybersecurity by rewarding the best practices with large tax deductions. It would also deter subpar practices through the required rating level posting on each company's site because companies will not want customers to see a poor cybersecurity rating. Second, the law would require all data breaches be posted on a company's website to deter companies from allowing repeated breaches. Finally, it would fine companies that violate customer privacy. Together, this law would regulate an unregulated industry and encourage companies to perform in the best interests of its customers.

CONCLUSION

The DTC genetic testing industry is growing, and as our knowledge of the effect of genetics on various aspects of who we are evolves, genetic testing will only become more widespread. But the current federal regulatory framework does not regulate the DTC genetic testing industry. Customers hand over their immutable genetic data and have little recourse when

levied a $148 million fine against Uber, a $230 million fine against British Airways, and a $275 million fine against Equifax for privacy violations. *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, F.T.C. (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

326. *See* Smith, *supra* note 322.

327. *See* Breslow, *supra* note 320.

that data is placed in unwanted hands. Security breaches cannot be avoided, but injured customers deserve to be recognized and compensated when breaches do occur, regardless of fault. This law is the first step in regulating a booming industry.

The proposed law has two main goals. First, it provides customers harmed by a data breach a private right of action under a strict liability theory, which will give the customer the best chance at compensatory recovery. Second, it grants the FTC authority to oversee and enforce regulations against DTC genetic testing companies, such that the companies are discouraged from the too common axiom of profits at all costs. This industry must be regulated because it handles immutable data. Such data must have a protection first, profit second outlook because a person's genetic code reveals more about that person than any other data.