Vanderbilt Journal of Entertainment & Technology Law

Volume 23 | Issue 3 Article 6

2021

Envisioning the FTC as a Facilitator of Blockchain Technology Adoption in the Direct-to-Consumer Genetic Testing Industry

Noah Spector

Envisioning the FTC as a Facilitator of Blockchain Technology Adoption in the Direct-to-Consumer Genetic Testing Industry

ABSTRACT

Seemingly overnight, the kingpins of the direct-to-consumer genetic testing (DTC-GT) industry shifted their focus from exploring their customers' DNA to commodifying it. Companies like Ancestry or 23andMe that were once exclusively known as mere sources of "infotainment" now regularly sell consenting customers' genetic data to pharmaceutical researchers or use it to develop drugs of their own. To gain these customers' consent, both firms employ a series of long, complex clickwrap contracts that largely fail to apprise their readers of the potential risks of sharing their genetic data. Nor do these agreements provide any form of compensation to those consumers whose data ultimately facilitates the development of a new, profitable drug.

Understandably, the relative autonomy major DTC-GT firms wield over their customers' genetic information—and the manner in which that autonomy is gained—raises serious privacy and bioethical concerns. More directly, it reflects a stark lack of federal oversight of the data management and storage practices of the DTC-GT industry as a whole. The emerging patchwork of state consumer privacy laws—while certainly more robust than any existing federal legislation—likewise falls short in fully protecting the privacy and dignitary interests of the DTC-GT consumers whose genetic data is shared and mined for profit.

This is not to say that DTC-GT consumers should be uniformly prohibited from contributing their genetic data to medicinal research. Such behavior should be encouraged to the extent this information can be transferred and stored securely. Nevertheless, the current exploitation of consumer data by major DTC-GT firms may, over the long term, inhibit medicinal progress by undermining demand for genetic testing and, thus, the pool of genetic data available for research. Accordingly, consumers and researchers alike would benefit from a more secure and equitable method of exchanging genetic information.

This Note argues that the recent advent of "blockchain genomics"—a form of exchange that allows consumers to securely loan

out their genetic information for research purposes in return for compensation—fits that bill. With mainstream DTC-GT firms unlikely to adopt such a system and no legislative solution on the horizon, this Note further suggests a role for the FTC, the country's de facto privacy regulator, to nudge major DTC-GT firms in that direction by exercising various tools of its soft regulatory authority.

TABLE OF CONTENTS

Over the last decade, titans of the direct-to-consumer genetic testing (DTC-GT) industry, such as 23andMe and Ancestry, have fashioned themselves into monolithic "banks" of genetic information.[1] These DNA-testing companies have adopted business models that prioritize the sale of consumer genetic data to third parties that seek to make advancements in medical research.[2] For example, pharmaceutical giant GlaxoSmithKline recently purchased a $300 million stake in 23andMe, providing the company access to 23andMe's trove of genetic data to develop new drugs.[3] Similarly, Ancestry partnered with Calico, a covert Google spin-off, to study aging and life extension.[4] All told, by

1. *See* Antonio Regalado, *More than 26 Million People Have Taken an At-Home Ancestry Test*, MIT TECH. REV. (Feb. 11, 2019), https://www.technologyreview.com/s/612880/more-than-26-million-people-have-taken-an-at-home-ancestry-test/ [https://perma.cc/AK9X-N8NY] ("By the start of 2019, more than 26 million consumers had added their DNA to four leading commercial ancestry and health databases, according to our estimates. If the pace continues, the gene troves could hold data on the genetic makeup of more than 100 million people within 24 months."); Cynthia McFadden, Aliza Nadi & Rich Schapiro, *DNA Test Company 23andMe Now Fueling Medical Research*, NBCNEWS (Jan. 17, 2019, 7:10 AM), https://www.nbcnews.com/health/health-news/dna-test-company-23andme-now-fueling-medical-research-n958651 [https://perma.cc/AFR2-7JJF] ("[N]o other gene bank . . . comes close to matching 23andMe's size.").

2. *See* Nicole Martin, *How DNA Companies like Ancestry and 23andMe Are Using Your Genetic Data*, FORBES (Dec. 5, 2018, 2:49 PM), https://www.forbes.com/sites/nicolemartin1/2018/12/05/how-dna-companies-like-ancestry-and-23andme-are-using-your-genetic-data/#15c1d8916189 [https://perma.cc/CXT3-85PG].

3. Jamie Ducharme, *A Major Drug Company Now Has Access to 23andMe's Genetic Data. Should You Be Concerned?*, TIME (July 26, 2018, 3:47 PM), https://time.com/5349896/23andme-glaxo-smith-kline/ [https://perma.cc/7JN5-LK9Z]. This is one of at least fourteen other partnerships 23andMe has established with a third party. ANDELKA M PHILLIPS, BUYING YOUR SELF ON THE INTERNET: WRAP CONTRACTS AND PERSONAL GENOMICS 131 (2019).

4. Erin Brodwin, *DNA-Testing Companies like 23andMe Sell Your Genetic Data to Drugmakers and Other Silicon Valley Startups*, BUS. INSIDER (Aug. 3, 2018, 10:45 AM),

systematically granting itself "the right to manage our genomic information, to store it, and to profit from it,"[5] the DTC-GT industry has reinvented itself as an intermediary in the genomic marketplace.[6]

Unsurprisingly, this development has led to a slew of privacy and bioethical concerns. Critics point out that permitting DTC-GT firms to wield centralized authority over genetic data—whether by housing it under one roof or sharing it with the highest institutional bidder—carries a host of increasingly novel and untenable consumer risks.[7] A single data breach resulting in the exposure of genetic information could, for example, subject affected consumers to certain forms of insurance discrimination,[8] military discharge,[9] or, one day, infiltration of their bank accounts.[10] Moreover, because DNA constitutes a potent human identifier that cannot be changed, both the consumer and her family may bear these risks for the rest of their lives.[11]

Separately, there is an emerging view that the DTC-GT industry's status as an intermediary in the genomic marketplace violates the basic dignitary and identity interests of DTC-GT customers.[12] Indeed, there is a compelling argument that the discrete

---

https://www.businessinsider.com/dna-testing-ancestry-23andme-share-data-companies-2018-8 [https://perma.cc/8L29-K392].

5. NIKOLAY KULEMIN, SERGEY POPOV & ALEXEY GORBACHEV, THE ZENOME PROJECT: WHITEPAPER 21 (2017), https://zenome.io/download/whitepaper.pdf [https://perma.cc/ME6H-7F5F].

6. That is, the emerging market between consumers—the producers and potential sellers of genetic information—and the researchers who wish to buy it. *See* Halil Ibrahim Ozercan, Atalay Mert Ileri, Erman Ayday & Can Alkan, *Realizing the Potential of Blockchain Technologies in Genomics*, 28 GENOME RSCH. 1255, 1261 (2018).

7. Paramount among the concerns related to data centralization are (i) that it may permit firms to "act[] as unnecessary mediator[s]" between the "owners" of genetic data (consumers) and its "users" (genetic researchers) and (ii) that centralized servers "create single points of failure both in terms of service availability and data privacy." Ozercan et al., *supra* note 6, at 1255.

8. *Can the Results of Direct-to-Consumer Genetic Testing Affect My Ability to Get Insurance?*, NAT'L INSTS. OF HEALTH, https://medlineplus.gov/genetics/understanding/dtcgenetic-testing/dtcinsurancerisk/ [https://perma.cc/B772-J4FM] (Sept. 18, 2020) [hereinafter *Insurance*].

9. Heather Murphy & Mihir Zaveri, *Pentagon Warns Military Personnel Against At-Home DNA Tests*, N.Y. TIMES (Dec. 24, 2019), https://www.nytimes.com/2019/12/24/us/military-dna-tests.html [https://perma.cc/6H2A-CV4V].

10. *See* PHILLIPS, *supra* note 3, at 52 (describing the increased adoption of voice recognition into the security systems of various banks).

11. *See* Ellen Wright Clayton, Barbara J. Evans, James W. Hazel & Mark A. Rothstein, *The Law of Genetic Privacy: Applications, Implications, and Limitations*, 6 J.L. & BIOSCIENCES 1, 7 (2019), https://academic.oup.com/jlb/article/6/1/1/5489401 [https://perma.cc/DY9X-YBYB].

12. Jessica L. Roberts, Theories of Genetic Ownership 51, 57 (Sept. 9, 2015) (unpublished manuscript) (on file with the Petrie-Flom Center for Health Law Policy, Biotechnology, and

sale of genetic data—solicited by firms like 23andMe for vaguely stated "scientific research purposes"—exploits well-intentioned consumers and defies their inherent right to benefit from information that is fundamentally *them*.[13] Ironically, this business model may undermine the long-term goals of the genetic research community: some researchers, for instance, fear that it increasingly disincentivizes would-be DTC-GT consumers from purchasing test kits, constraining the pool of available genetic information.[14] Affording consumers the right to own and sell their information, they claim, is the best method of ensuring the information's long-term flow.[15]

The recent advent of "blockchain genomics" may provide the best model for remedying this array of concerns.[16] A blockchain—defined broadly as a highly secure, decentralized data storage system—can allow its users to effectively "own" the data they generate. To that end, start-up genomic sequencing companies like Nebula Genomics have begun to utilize their own custom blockchain networks to provide customers with virtually the same services as DTC-GT companies, while also granting them sole ownership, access, and control over their data in an extremely secure fashion.[17] Notably, these consumers may choose to anonymously sell or rent their information to researchers or pharmaceutical companies.[18]

Because major DTC-GT companies have no real incentive to adopt blockchain systems of their own (and are unlikely to encounter one any time soon), this Note argues that the Federal Trade Commission (FTC) should nudge them in that direction.[19] Specifically, it recommends that the FTC (i) exercise its repertoire of informational

---

Bioethics at Harvard Law School), https://petrieflom.law.harvard.edu/assets/publications/Roberts_Genetic_Ownership_Draft.pdf [https://perma.cc/K4MT-2U79].

13. *See* Clayton et al., *supra* note 11, at 17–18; Roberts, *supra* note 12, at 57. This view roots itself in the principle of "genetic exceptionalism"—the idea that genetic information is so highly personal that it merits special treatment relative to other forms of personal data. *See id.*

14. *See* Dennis Grishin, Kamal Obbad, Preston Estep, Kevin Quinn, Sarah Wait Zaranek, Alexander Wait Zaranek, Ward Vandewege, Tom Clegg, Nico César, Mirza Cifric & George Church, *Accelerating Genomic Data Generation and Facilitating Genomic Data Access Using Decentralization, Privacy-Preserving Technologies and Equitable Compensation*, 1 BLOCKCHAIN IN HEALTHCARE TODAY, no. 1, 2018, at 1, 3–4.

15. *See id.* at 5–6.

16. Helen Albert, *How Blockchain Companies Are Helping Us Protect Our Genomic Data*, LABIOTECH.EU (June 26, 2019), https://www.labiotech.eu/genomics/blockchain-control-genomic-data/ [https://perma.cc/S3CR-5NHR].

17. Frost & Sullivan, *Blockchain Technology Empowering Genetics*, ALL. OF ADVANCED BIOMEDICAL ENG'G (2018), https://aabme.asme.org/posts/blockchain-technology-empowering-genetics [https://perma.cc/4472-92JP].

18. Albert, *supra* note 16.

19. *Infra* Part IV.

resources—including its newfound "Blockchain Working Group"—to educate consumers, researchers, and firms on the utility of blockchain technology as a management system for genetic data and (ii) craft voluntary standards that promote its adoption. Part I lays out both the function of the DTC-GT industry and its reliance on self-regulation to govern its use of genetic data. Part II assesses how this system of self-governance perpetuates the privacy and bioethical issues previously described, and Part III explains why blockchain systems may serve as the most effective method of confronting them. Part IV diagrams the two-pronged strategy the FTC should employ to facilitate the DTC-GT industry's adoption of blockchain technologies and offers concluding remarks.

I. THE DTC-GT INDUSTRY'S LEGAL LANDSCAPE AND INHERENT PRIVACY CONCERNS

A. The DTC-GT Industry at a Glance

1. Present and Future State of the DTC-GT Market

There are roughly ninety private, US-based DTC-GT companies which offer four general categories of services: family relationship, ancestry and genealogy, lifestyle and wellness, and health.[20] The process underpinning these services is fairly uniform: consumers purchase a test kit and, once the kit is received, submit a sample of genetic material (generally saliva) in return.[21] After the test is analyzed, the firm conveys its results to the consumer, usually via an online platform.[22] Based on their findings, some DTC-GT firms may offer their users continual health or ancestry updates as their respective databases grow.[23]

Overall, the DTC-GT industry is now largely oriented toward providing ancestry- and relationship-focused products, although predictive tests—which indicate an individual's genetic predispositions and risks for certain diseases—continue to increase in popularity.[24]

---

20. 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, 47 (2018).

21. PHILLIPS, *supra* note 3, at 13.

22. *Id.* at 13.

23. *Id.*

24. Clayton et al., *supra* note 11, at 16–17; *see* Megan A. Allyse, David H. Robinson, Matthew J. Ferber & Richard R. Sharp, *Direct-to-Consumer Testing 2.0: Emerging Models of Direct-to-Consumer Genetic Testing*, 93 MAYO CLINIC PROC. 113, 119 (2018), https://www.mayo-clinicproceedings.org/action/showPdf?pii=S0025-6196%2817%2930772-3.

This shift marks the industry's rapid transformation from a source of "infotainment" (i.e., entertainment-driven information) to a private provider of legitimate health-like services[25] and is largely attributable to (i) the Food and Drug Administration's (FDA) newly relaxed approach to predictive testing,[26] (ii) the decreasing costs of genomic sequencing,[27] and (iii) the increasing ease in which genetic data is shared.[28]

By increasing the scope and accessibility of their services over the past ten years, DTC-GT firms have exponentially expanded their general market.[29] For example, industry kingpins like 23andMe grew from one hundred thousand to twelve million total customers within this period of time.[30] Such growth has enabled the four leading US DTC-GT firms (23andMe, Ancestry, FamilyTreeDNA, and MyHeritage) to aggregate the genetic information of more than twenty-six million individuals—a pool of information large enough to identify at least a majority of Americans with European descent.[31] By 2021, that same pool is projected to contain the genetic code of roughly one hundred million people.[32] Notwithstanding this projected growth, it should be noted that major firms like 23andMe have hit a slow period, potentially due to increasing concern amongst consumers regarding the privacy of

25. *See* Allyse et al., *supra* note 24, at 113–14, 119. *But see* Grishin et al., *supra* note 14, at 3 (stating that, at present, DTC-GT consumers are primarily interested in "infotainment"). This growth is largely owed to the FDA's landmark decision to authorize 23andMe to "market a carrier test for Bloom Syndrome in 2015." Clayton et al., *supra* note 11, at 16.

26. *See* Clayton et al., *supra* note 11, at 16. Soon after, the agency announced its intention to exempt 23andMe's "Genetic Health Risk" tests from premarket review in order to provide "other, similar tests to enter the market as quickly as possible and in the least burdensome way." *Id.* at 17. The firm, capitalizing on the FDA's receptiveness, now markets tests for fourteen different conditions, including Parkinson's and Alzheimer's disease. *DNA Reports List*, 23ANDME, https://www.23andme.com/dna-reports-list/ [https://perma.cc/3AEM-LHHW] (last visited Jan. 28, 2021).

27. Grishin et al., *supra* note 14, at 2.

28. *See* Kim Hart, *Genetic Testing Firms Share Your DNA Data More than You Think*, AXIOS (Feb. 25, 2019), https://www.axios.com/dna-test-results-privacy-genetic-data-sharing-4687b1a0-f527-425c-ac51-b5288b0c0293.html [https://perma.cc/CA5C-AG8B].

29. *See* Hazel & Slobogin, *supra* note 20, at 37 n.5 ("The market value of the US DTC . . . industry grew from a humble $15 million in 2010 to over $210 million in 2017 and is projected to reach $350 million by 2020.").

30. *History*, 23ANDME, https://mediacenter.23andme.com/assets/timeline/index.html [https://perma.cc/AQ72-CVQR] (last visited Jan. 28, 2021); *About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us/ [https://perma.cc/DS3T-UVU2] (last visited Jan. 28, 2021).

31. Regalado, *supra* note 1; 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 [https://perma.cc/NPA2-9HP6].

32. Regalado, *supra* note 1.

their data.[33] Nevertheless, the velocity of these firms' rise begs two questions: what genetic information are consumers increasingly relinquishing to DTC-GT firms, and what could happen if that information falls into the wrong hands?

2. How DTC-GT Firms Process Genetic Data (and How That Might Change)

Generally, there are two methods of processing a genetic test: genotyping and sequencing.[34] Genotyping takes a figurative snapshot of a specific part of a donor's genome to identify any number of predetermined genetic variants that are associated with certain traits, characteristics, and diseases.[35] Sequencing, on the other hand, is much more comprehensive insofar as it may be used to identify those same known *and* unknown variants unique to a single donor by analyzing entire or specific strands of DNA.[36] To highlight this difference in scope, it may be helpful to think of the letters that comprise our genetic code as "words on a [book] page, telling a story, chapter by chapter."[37] Genotyping is akin to processing a patchwork of random, scattered words; sequencing, on the other hand, can effectively process entire chapters.[38]

Notwithstanding the greater amount of genetic information that sequencing can derive, market-leading DTC-GT firms like 23andMe exclusively rely on genotyping to process genetic samples, largely on the belief that sequencing—in light of its cumbersome, lengthy, and expensive nature—is simply not necessary to satisfy consumer

33. Daniel Roberts, *Once-Hot DNA Testing Unicorn 23andMe Is in Serious Trouble*, YAHOO FIN. (Jan. 29, 2020), https://finance.yahoo.com/news/oncehot-dna-testing-unicorn-23-and-me-is-in-serious-trouble-115817212.html [https://perma.cc/MT2A-4KMC].

34. *See What Is Genotyping?*, THERMOFISHER SCI., https://www.thermofisher.com/us/en/home/life-science/pcr/real-time-pcr/real-time-pcr-learning-center/genotyping-analysis-real-time-pcr-information/what-is-genotyping.html [https://perma.cc/D47A-4QMY] (last visited Oct. 31, 2019).

35. *Id.*

36. *Genotyping vs. Sequencing: What's the Difference?*, ORIG3N, https://orig3n.com/blog/genotyping-vs-sequencing-whats-the-difference/ [https://perma.cc/3ZFF-UFC8] (last visited Oct. 31, 2019).

37. Elissa Levin, *DNA Technologies 101: Genotyping vs. Sequencing, and What They Mean for You*, HELIX: RSCH. BLOG (Aug. 4, 2017), https://blog.helix.com/dna-technologies-genotyping-vs-sequencing/ [https://perma.cc/JS4X-NCGZ].

38. *Id.*

demand.[39] That justification may be short-lived.[40] For one, the price of whole-genome sequencing—a process that initially cost $2.7 billion and now gravitates around $1,000—continues to decrease.[41] Moreover, as described, a growing number of companies have begun to offer complex and comprehensive health tests that require data that is more conveniently obtainable through sequencing.[42] Finally (and perhaps most importantly), sequenced genomic data is, in light of its breadth, significantly more valuable to third-party researchers and pharmaceutical companies than genotyped data.[43] It stands to reason, then, that these third parties would pay even more than they already do to access this information.[44] Major firms like 23andMe and Ancestry that have experienced a decline in revenue would, logically, find such an offer highly appealing.[45] Indeed, Ancestry recently announced the launch of a sequencing tool meant to inform consumers of their underlying health risks.[46]

All told, these developments signal that major firms may soon adopt sequencing processes to accommodate their individual and institutional patrons, increasing the amount of genetic information they store and traffic.[47] As mainstream DTC-GT firms increasingly use sequencing services, the corresponding privacy risks associated with patronizing them will grow.

---

39. *See Difference Between DNA Genotyping & Sequencing*, 23ANDME, https://customer-care.23andme.com/hc/en-us/articles/202904600-Difference-Between-DNA-Genotyping-Sequencing (last visited on Oct. 31, 2019).

40. *See, e.g.*, Frost & Sullivan, *supra* note 17 (projecting 15 percent of the global population to sequence their DNA by 2025).

41. Megan Molteni, *Now You Can Sequence Your Whole Genome for Just $200*, WIRED (Nov. 19, 2018, 8:00 AM), https://www.wired.com/story/whole-genome-sequencing-cost-200-dollars/ [https://perma.cc/8TLP-F2WV] (covering one genome sequencing company that offered its services for $199). Even the more expensive sequencing services occasionally offer a promotional discount to "send[] a clear signal . . . that the $99 genome will be here in three to five years." *Id.*

42. Hazel & Slobogin, *supra* note 20, at 63.

43. *See* Grishin et al., *supra* note 14, at 2 (describing how genotyping is generally less valuable to researchers because it "does not allow [for the] discovery of novel variants, including those that cause disease").

44. *See* Sarah Watts & Kristen Hovet, *Your Genetic Data Is the New Oil. These Startups Will Pay to Rent It.*, LEAPSMAG (Sept. 21, 2018), https://leapsmag.com/your-genetic-data-is-the-new-oil-these-startups-will-pay-to-rent-it/ [https://perma.cc/G7ND-DWZ5] (detailing the recent series of lucrative DTC-GT partnerships involving third-party researchers and their underlying desire to access better, less-restricted data).

45. Roberts, *supra* note 12, at 55.

46. Christina Farr, *Ancestry to Lay Off 6% of Workforce Because of a Slowdown in the Consumer DNA-Testing Market*, CNBC, https://www.cnbc.com/2020/02/05/ancestry-layoffs-of-6percent-100-people-amid-dna-test-slowdown.html [https://perma.cc/T42W-LNYC] (Feb. 5, 2020, 5:40 PM).

47. Hazel & Slobogin, *supra* note 20, at 63.

B. Risks of Sharing Genetic Data

The current privacy risks associated with consuming DTC-GT services are forthright. Major firms like 23andMe, as with any firm that stores personal data, openly admit their security systems can be breached.[48] Few realize, however, how catastrophic this could be.[49] In the event of a breach, leaked genetic information could be used by non-health insurers (i.e., disability insurers, long-term care insurers, or life insurers) or lenders to discriminate against policyholders or loan applicants;[50] by foreign countries seeking to exploit national security vulnerabilities (e.g., by leveraging a high-up US official's predisposition to a certain disease as blackmail);[51] by law enforcement to prosecute genetic donors (or their families);[52] or for mass surveillance purposes.[53]

Some of those scenarios may not appear pressing. Permitting law enforcement, for example, to cross-reference crime scene DNA with publicly available genetic data—a practice already used to catch criminals like the notorious Golden State Killer[54]—may seem desirable. That assumes, however, that the genetic data used on either end of the cross-referencing is genuine, which is not guaranteed. As technology evolves, it grows increasingly likely that genetic data may be used to emulate and steal another person's identity, allowing nefarious actors, for example, to use synthetic DNA to frame another person for a crime.[55]

---

48. *See, e.g.*, *Privacy Policy*, 23ANDME, https://www.23andme.com/about/privacy/ [https://perma.cc/XZ3V-GP6S] (Oct. 30, 2020) ("[W]e cannot guarantee the confidentiality and security of your information due to the inherent risks associated with storing and transmitting data electronically.").

49. Amy Brown, *DNA Testing Is Popular, but Many Are Unaware of Privacy Concerns*, TRIPLEPUNDIT (Dec. 18, 2018), https://www.triplepundit.com/story/2018/dna-testing-popular-many-are-unaware-privacy-concerns/55936 [https://perma.cc/N39D-RU39] ("There is almost a complete lack of awareness among the public about [these] issue[s] . . . [instead, t]he DNA kits are being viewed as stocking stuffers or cocktail party conversation.").

50. *Insurance*, *supra* note 8; *Hack of DNA Website Exposes Data from 92 Million Accounts*, THE DIGIT. AGE BLOG (June 7, 2018), http://www.thedigitalageblog.com/cyber-security/hack-of-dna-website-exposes-data-from-92-million-accounts/ [https://perma.cc/ZZ26-TTZT].

51. *See* Murphy & Zaveri, *supra* note 9.

52. PHILLIPS, *supra* note 3, at 152.

53. Shawn Snow, *Pentagon Advises Troops to Not Use Consumer DNA Kits, Citing Security Risks*, MIL. TIMES (Dec. 24, 2019), https://www.militarytimes.com/2019/12/24/pentagon-advises-troops-to-not-use-consumer-dna-kits-citing-security-risks/ [https://perma.cc/6FBZ-3UB4] ("[T]here is increased concern in the scientific community that outside parties are exploiting the use of genetic data for questionable purposes, including mass surveillance and the ability to track individuals without their authorization or awareness.").

54. Gina Kolata & Heather Murphy, *The Golden State Killer Is Tracked Through a Thicket of DNA, and Experts Shudder*, N.Y. TIMES (Apr. 27, 2018), https://www.nytimes.com/2018/04/27/health/dna-privacy-golden-state-killer-genealogy.html [https://perma.cc/UC2C-69RS].

55. PHILLIPS, *supra* note 3, at 52.

Indeed, biometric information (such as fingerprints) is already at risk of being used by criminal organizations to infiltrate private bank accounts.[56]

While some consumers may consider these scenarios to be remote problems, two points bear emphasis: because DNA is immutable and a potent human identifier, it renders any victim of genetic fraud perpetually helpless to seen and unforeseen uses by bad actors;[57] and likewise it implicates family members who share the same genetic code.[58] Thus, should genetic data fall into the wrong hands, individuals who never actually consented to genetic testing in the first place may be rendered indefinitely vulnerable to attack.

C. Informed Consent: Nonexistent or a Virtual Fiction in the DTC-GT Industry

1. Privacy Policies as a Mechanism of Self-Governance

As elaborated in Section I.D, there is no meaningful federal oversight of the DTC-GT industry's management of consumer data.[59] Accordingly, clickwrap agreements now serve as the industry's exclusive governance mechanism.[60] Such agreements, in a nutshell, are digitized contracts of adhesion that bind the consumer after she indicates notice and consent by the click of a button (i.e., "I agree").[61] Notably, clickwrap agreements need not display those terms on the same page as the button used to indicate consent in order for the provider to give proper notice; embedding a digital link will likely suffice.[62]

---

56. *Id.*

57. *See* Clayton et al., *supra* note 11, at 7; Martin, *supra* note 2 ("[A] DNA leak would be much worse than a credit leak because simply, you cannot change your DNA.").

58. Hazel & Slobogin, *supra* note 20, at 43; Rachele M. Hendricks-Sturrup & Christine Y. Lu, *Direct-to-Consumer Genetic Testing Data Privacy: Key Concerns and Recommendations Based on Consumer Perspectives*, J. PERSONALIZED MED., June 2019, at 1, 2 (2019) (noting the New Jersey attorney general's 2017 warning to Ancestry customers that DNA information "may be used against 'you or a genetic relative'").

59. *See* Hazel & Slobogin, *supra* note 20, at 40 ("[T]hese laws generally do not directly implicate the bulk of the DTC-GT industry[.]"). The lack of a regulatory response may also stem from the DTC-GT industry's inability to "fit neatly into existing legal categories" because it frames health and biological tests as consumer services. PHILLIPS, *supra* note 3, at 27.

60. PHILLIPS, *supra* note 3, at 28.

61. Hazel & Slobogin, *supra* note 20, at 38; *see also* PHILLIPS, *supra* note 3, at 28.

62. MARGO H.K. TANK & DAVID WHITAKER, THE EFFECTIVENESS OF CLICKWRAP FOR LEGALLY ENFORCEABLE AGREEMENTS. 4–5 (2019), https://www.docusign.com/sites/default/files/the_effectiveness_of_clickwrap_for_legally_enforceable_agreements_0.pdf [https://perma.cc/2FSW-H8LM].

Critics argue that allowing DTC-GT firms to draft and conceal their own terms behind a hyperlink impedes the consumer's ability to understand the consequences of purchasing a test kit.[63] The standard response of a DTC-GT firm, of course, would be that once it provides the consumer with sufficient notice of its terms, it can do no more; it is her obligation—at least legally—to actually read the agreement.[64] This, as described in Section I.C.2, ignores the fact that some consumers may lack the skills or scientific background to truly grasp the consequences of the agreement.[65] Moreover, it fails to acknowledge the relative abundance of DTC-GT firms which either do not provide consumers any privacy terms or leave out crucial information within their agreements.[66]

Indeed, in a survey of all ninety US-based DTC-GT companies, thirty-five neglected to provide a privacy policy, leaving consumers in the dark as to how their "genetic data was collected, used, or shared."[67] Of the fifty-five firms found to offer a policy, only five allow consumers to delete all of their data;[68] forty do not discuss ownership of genetic material or the data resulting from its analysis;[69] forty-nine vaguely commit to keeping consumer genetic data secure (as opposed to the seventeen that specifically note their use of encryption);[70] fifty-two provide "no information regarding how the company would deal with a security breach or whether an affected consumer would be notified;"[71] and twenty-three indicate that data may be shared with third parties with or without express consent.[72] Finally, "almost all companies" maintain the ability to change their privacy policy "at any time," often without having to notify the consumer.[73]

2. Lack of Transparency and the Problem of (Un)Informed Consent

Despite the DTC-GT industry's general reluctance to publicly state clear privacy terms (or any terms at all), studies suggest DTC-GT

63. PHILLIPS, *supra* note 3, at 28; Hazel & Slobogin, *supra* note 20, at 38.

64. *See* Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1176 (9th Cir. 2014) ("Courts have also been more willing to find the requisite notice for constructive assent where the . . . user is required to affirmatively acknowledge the agreement before proceeding with use of the website.").

65. *Infra* Section I.C.2.

66. Hazel & Slobogin, *supra* note 20, at 48.

67. *Id.* at 48.

68. *Id.* at 51.

69. *Id.* at 52.

70. *Id.* at 53.

71. *Id.* at 53.

72. *Id.* at 55.

73. *Id.* at 57.

consumers "feel[] relatively well-informed about the privacy implications of purchasing a genetic test."[74] This discrepancy might be explained by the unusually comprehensive policies offered by the handful of market-dominating firms—namely, 23andMe and Ancestry.[75] Both firms, for example, go so far as to require informed consent to share a consumer's individual-level data with third parties;[76] allow users to delete their account information;[77] claim to share only "de-identified" or "aggregated" individual-level data that is stripped of personal identifiers;[78] and vaguely commit to maintaining "industry standard" or "comprehensive" encryption software subject to independent security certification and continual audit.[79]

While these assurances exceed industry norms, they still fall short of fully addressing extant consumer privacy concerns. For one, requiring informed consent to share genetic data may simply not be an adequate way of informing or protecting an individual's interest in her genetic privacy.[80] Of the roughly eight million 23andMe consumers who have consented to sharing their genetic data,[81] some may lack the literacy skills to fully comprehend the complex terms in front of them.[82] Others may fail to foresee the full gambit of consequences attached to the potential leakage of their genetic data,[83] or, as is the habit of 90 percent of US consumers, might simply skim or skip the terms entirely.[84] Even those who actually read and comprehend these terms

74. Emily Christofides & Kieran O'Doherty, *Company Disclosure and Consumer Perceptions of the Privacy Implications of Direct-to-Consumer Genetic Testing*, 35 NEW GENETICS & SOC'Y 101, 117 (2016). Many consumers, for example, wrongly assumed that their genetic sample would be destroyed after testing. *Id.*

75. Hazel & Slobogin, *supra* note 20, at 44, 63; Christofides & O'Doherty, *supra* note 74, at 117–18.

76. *Individual Data Sharing Consent*, 23ANDME, https://www.23andme.com/about/individual-data-consent/ [https://perma.cc/3HAY-36GE] (last visited Jan. 15, 2020); *see Your Privacy*, ANCESTRY, https://www.ancestry.com/cs/legal/privacystatement [https://perma.cc/3NER-DZVV] (last visited Jan. 28, 2021).

77. *Privacy Policy*, *supra* note 48; *Your Privacy*, *supra* note 76.

78. *Privacy Policy*, *supra* note 48; *Your Privacy*, *supra* note 76.

79. *Privacy Policy*, *supra* note 48; *Your Privacy*, *supra* note 76.

80. Christofides & O'Doherty, *supra* note 74, at 118.

81. *See 23andMe for Scientists*, 23ANDME, https://web.archive.org/web/20200222214128/https://research.23andme.com/ (last visited Feb. 22, 2020) (claiming over 10 million kits sold, and that "80% of customer's consent to research").

82. Hendricks-Sturrup & Lu, *supra* note 58, at 2.

83. *See supra* Section I.B (discussing the risks of genetic exposure).

84. Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017, 6:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/BX9Z-92RL]. In the DTC-GT context, this may be attributed to the consumer assuming a false sense of security by the

of consent are still kept in the dark as to how their genetic data will be shared. Neither 23andMe nor Ancestry, for example, obligate themselves to inform consenting consumers when their data is shared, where it is sent, how it will be protected by the recipient, and whether or not it can be retrieved upon the consumer's request.[85] Customers of these firms also go unwarned that their de-identified genetic data may be reidentified.[86] Collectively, these deficiencies suggest that a customer of either firm who consents to sharing her data for research purposes effectively relinquishes control, perhaps permanently, over her own genetic profile, precluding her from acting on a future change of heart and increasing her or her relatives' risk of genetic identification.

Additionally, both 23andMe and Ancestry require consumers to send their genetic samples to independent genotyping lab facilities (which analyze and store genetic information) without further consent.[87] These labs—seemingly defying consumer expectations[88]— retain user data for "regulatory compliance purposes," even after they issue a request for its deletion.[89] No information related to these facilities' data management or security practices is provided in either company's privacy policy.[90] Thus, to some degree, even standard DTC-GT consumers risk genetic exposure.

3. General Security Concerns

While DTC-GT consumers may feel well informed about their general privacy rights, they nonetheless appear squeamish about how

---

mere presence of an informed consent requirement. *See* Christofides & O'Doherty, *supra* note 74, at 118 ("[C]onsumers often mistake the *presence* of a privacy policy for the *protection* of privacy.").

85. *See Privacy Policy*, *supra* note 48 (demonstrating a lack of any of these protections in 23andMe's privacy policy).

86. Hazel & Slobogin, *supra* note 20, at 44. To "re-identify" de-identified genetic data, a malicious actor need only identify certain personal traits (i.e., eye and hair color) noted within the data and "cross-reference those traits against publicly-available demographic data to identify the donor." Brown, *supra* note 49.

87. *See Privacy Policy*, *supra* note 48 (stating the consumer's obligation to ship her saliva sample to a 23andMe-controlled processing center or a certified third-party laboratory); *Your Privacy*, *supra* note 76 (stating the company's general practice of processing consumer DNA samples at one of its several independent laboratory partners).

88. *See* Christofides & O'Doherty, *supra* note 74, at 115 ("With regard to DNA samples, the most common response was that participants expected it to be destroyed after testing.").

89. 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?login=smartlock&auth=login-smartlock [https://perma.cc/HN7R-5639].

90. *Privacy Policy*, *supra* note 48; *Your Privacy*, *supra* note 76.

their data is actually secured and protected.[91] This is likely due in part to the string of recent "electronic health record breaches" that implicated half of the US population, or the handful of DTC-specific breaches that have occurred—one of which resulted in the exposure of the personal (nongenetic) data of ninety-two million users.[92] Indeed, malicious actors are successfully targeting privately stored health information at a record pace.[93] While these efforts have largely concentrated on hospitals and other health care providers,[94] the growing value of genetic data may render the genetic testing and research industries increasingly appealing targets for future breach attempts.[95]

Given the incredibly vague nature in which major DTC-GT firms describe their information security systems, gauging the likely success of an attempted breach of any given firm's data storage system is difficult.[96] Because the use of third-party cloud storage and strong encryption software appears to be the norm,[97] and, as some firms readily admit, such systems are not invulnerable to being hacked,[98] the breach of a DTC-GT firm is at least plausible.[99] Moreover, as 23andMe

91. *See* Hendricks-Sturrup & Lu, *supra* note 58, at 5 (citing several studies that demonstrate a widespread consumer belief that genetic data could be "easily hacked").

92. *Id.*; Marcus Baram, *The FTC Is Investigating DNA Firms like 23andMe and Ancestry over Privacy*, FAST CO. (June 5, 2018), https://www.fastcompany.com/40580364/the-ftc-is-investigating-dna-firms-like-23andme-and-ancestry-over-privacy [https://perma.cc/D5KD-CTHW] (discussing the breach of MyHeritage, an Israeli-based DTC-GT firm).

93. Waldemer W. Koczkodaj, Mirosław Mazurek, Dominik Strzałka, Alicja Wolny-Dominiak & Marc Woodbury-Smith, *Electronic Health Record Breaches as Social Indicators*, 141 SOC. INDICATORS RSCH. 861, 870 (2018) ("[S]tatistical evidence shows that data breaches of electronic health records have taken place at an unprecedented scale.").

94. *Id.* at 862.

95. *See id.* at 869 (discussing the unique appeal of health information—which stems particularly from its immutability—to malicious actors who may seek to exploit it for financial gain). An attacker may, for example, wish to sell the genetic data back for ransom, or discretely sell it to unscrupulous insurance companies. Angela Chen, *Why a DNA Data Breach Is Much Worse than a Credit Card Leak*, THE VERGE (June 6, 2018, 3:54 PM), https://www.theverge.com/2018/6/6/17435166/myheritage-dna-breach-genetic-privacy-bioethics [https://perma.cc/G6LN-YAZA].

96. *Supra* Section I.C (discussing the pitfalls of DTC-GT privacy policies).

97. *See* Grishin et al., *supra* note 14, at 7 ("Storage and processing of genomic data has moved from local servers to remote clouds."); *Privacy Policy*, *supra* note 48.

98. *Privacy Policy*, *supra* note 48 ("[W]e cannot guarantee the confidentiality and security of your information due to the inherent risks associated with storing and transmitting data electronically.").

99. Koczkodaj et al., *supra* note 93, at 869.

recently demonstrated by sending the wrong test results to ninety-six customers, firms are always prone to simple human error.[100]

D. Legislative Attempts to Regulate the DTC-GT Industry

1. The Absence of Effective Federal Law

Existing areas of DTC-GT-related federal law almost uniformly govern devices and test kits marketed by DTC-GT companies, not the genetic information they are used to collect.[101] Those laws which implicate genetic data—namely, the Health Insurance Portability and Accountability Act (HIPAA) and the Genetic Information Non-Discrimination Act (GINA)—do not enforce any security or privacy norms in the DTC-GT industry.[102]

HIPAA grants the Department of Health and Human Services the power to regulate the disclosure of "health information."[103] Yet, because HIPAA only applies to health care providers "or those who pay for it (such as insurers)" and not private entities who collect health-related information,[104] the statute is largely inapplicable in the DTC-GT context.[105] Moreover, even if DTC-GT firms fell within its purview, HIPAA's exclusion of de-identified health information means it would hardly impact data-sharing practices among major firms like 23andMe, which exclusively share de-identified (but perhaps re-identifiable) genetic data.[106]

---

100. Jason Kincaid, *23andMe Sends Wrong DNA Test Results to 96 Customers*, TECHCRUNCH (June 7, 2010, 10:24 PM), https://techcrunch.com/2010/06/07/23andme-sends-wrong-dna-test-results-to-96-customers/ [https://perma.cc/A77P-UFSS].

101. PHILLIPS, *supra* note 3, at 19, 27 (positing that "the most likely area of existing law" applicable to the DTC-GT industry is "the regulation of medical devices" and that "[o]verall there is a general lack of specific regulation for the DTC[-GT] industry globally" in light of its disruptive quality).

102. Clayton et al., *supra* note 11, at 10–14.

103. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C. (2018)). HHS followed this statutory mandate by promulgating the Privacy Rule. 45 C.F.R. pts. 160, 164 (2019). The Privacy Rule "establishes national standards to protect individuals' medical records and other personal health information." *The HIPAA Privacy Rule*, U.S. DEP'T OF HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/index.html [https://perma.cc/555V-MRDE] (Dec. 10, 2020).

104. Clayton et al., *supra* note 11, at 14.

105. *Id.*

106. *Id.* at 12 ("The Privacy Rule also has glaring gaps in its framework for keeping people informed about who has been given access to their genetic information. For example, when a person's genetic information is disclosed in a deidentified format, the Privacy Rule[] . . . [does] not require covered entities to tell the individual about the disclosure, even though deidentified genetic

GINA's primary purpose is to prohibit employers and health insurers from discriminating against employees or the insured based on genetic information.[107] While the statute extends the definition of "health information" to include "genetic information,"[108] GINA is significantly weakened by its exclusion of non-health insurers, which enables disability, long-term care, and life insurers "the right to request medical information, including the results of any genetic testing, when making decisions about coverage and rates."[109]

2. Assessing State-Level Genetic Privacy Laws

In the absence of effective federal law, nearly every state has enacted genetic privacy laws that differ in applicability and stringency.[110] Of those, twenty-six states provide citizens a private right of action as a method of enforcement.[111] Two of those states—Alaska and Nevada—have enacted the most "exemplary" laws.[112] Alaska's law stands out for its comprehensiveness; it requires, for instance, "informed and written consent" to collect, analyze, and retain information related to an individual's DNA and recognizes (albeit vaguely) a person's property right to their genetic information.[113] It also permits citizens to recover up to $100,000 from any entity whose violation of the law "resulted in profit or monetary gain to the violator."[114] Yet, notably, the law does not grant the individual a right to control access to her genetic data,[115] nor does it address how her supposed property right affects the sale of her information to a third party.[116]

Nevada's genetic privacy law is a little more thorough. It requires the same level of informed consent for all genetic testing but

---

information is potentially reidentifiable."). The Privacy Rule is also said to fail consumer interests by precluding individuals whose information is shared from legal action. *Id*. at 14.

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

108. 45 C.F.R. § 160.103.

109. *Insurance*, *supra* note 8.

110. Clayton et al., *supra* note 11, at 12.

111. 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, 64 (2019).

112. *State Genetic Privacy Policy*, ELEC. PRIV. INFO. CTR., https://epic.org/state-policy/genetic-privacy/ [https://perma.cc/8H3P-HM62] (last visited Oct. 31, 2019).

113. ALASKA STAT. § 18.13.010 (2004).

114. ALASKA STAT. § 18.13.020.

115. *State Genetic Privacy Policy*, *supra* note 112.

116. *Id.*

also provides consumers with the ability to "inspect or obtain" their genetic information at any time and a guarantee that all genetic information "received for the purpose of a study [will] be destroyed upon the study's completion or the donor's withdrawal."[117] This mandatory erasure requirement allows consumers to revoke consent to having their data shared. However, as with Alaska, it is unclear whether this right applies to third parties who already received the data.

The California Consumer Privacy Act (CCPA), the first state-level comprehensive data privacy law, perhaps comes the closest to addressing modern DTC-GT-related privacy concerns.[118] Though not specifically aimed at protecting genetic information, the Act guarantees, among other provisions, four pertinent privacy rights to California citizens: (i) the right to be explicitly informed whether their personal information will be collected or shared;[119] (ii) the right to know if and why their personal information has been shared with a specific category of third party in the past twelve months;[120] (iii) the right to have their personal information deleted by the collecting business and its service providers (but not third-party partners);[121] and (iv) the right to sue that business if, in the aftermath of a security breach which stems from its failure to "implement and maintain reasonable security procedures and practices," their personal information is stolen or disclosed.[122]

All told, the patchwork of state genetic privacy laws has created a "web of protection" that extends HIPAA-like obligations to DTC-GT firms.[123] This, in turn, has spurred major DTC-GT firms to implement uniform privacy practices not required by federal law—namely, mandating a consumer's informed consent to share genetic data with third parties. However, even informed consent requirements, as noted in Section I.C, are unlikely to sufficiently protect the privacy interests of DTC-GT consumers.[124] Providing consumers with the right to have their genetic data deleted by *any* private entity who possesses it would, theoretically, be enough to offset this shortcoming. Nevertheless, no state—including Nevada and California—goes that far. Moreover, even if certain states were to adopt such a law, only their citizens would be

117. NEV. REV. STAT. § 629.161 (2015).
118. CAL. CIV. CODE §§ 1798.100–.199 (2018).
119. CAL. CIV. CODE § 1798.120.
120. CAL. CIV. CODE § 1798.130.
121. CAL. CIV. CODE § 1798.105.
122. CAL. CIV. CODE § 1798.150.
123. Wolf et al., *supra* note 111, at 44.
124. *Supra* Section I.C.

able to enforce it. To that end, a uniform, federal approach—which, as this Note advocates, should be spearheaded by the FTC—is desirable.

II. BIOETHICAL ISSUES MANIFESTED BY DTC-GT SELF-REGULATION

A. Ownership of Genetic Data and the Need for Equitable Compensation

1. The Genetic Ownership Debate: Labor and Personhood Theories

Several competing ideologies over the ownership of genetic data exist.[125] Members of the biotech industry, for example, adopt a "labor theory" approach, which asserts that the efforts expended by researchers and employees in the processing and production of genetic data effectively qualifies it as a form of company property.[126] They point to current US common law as set forth in *Moore v. Regents of the University of California*, which does not recognize an individual's property right in their "excised cells,"[127] as support for their view. Moreover, they vigorously emphasize that to afford individuals' ownership rights would effectively strip the scientific community of its economic incentives, ossifying medical progress.[128]

Consumer advocates, on the other hand, adopt a "personhood" approach, which rests on the natural intuition that humans inalienably own the information that defines their existence.[129] To afford private entities the ability to sell genetic data, they hold, merely incentivizes the violation of fundamental identity and dignitary interests.[130] They also highlight that US common law has yet to extend *Moore* to the genetic information contained *within* a human's "excised cells."[131]

---

125. Roberts, *supra* note 12, at 4–6.

126. *Id.* at 6.

127. *Id.* at 46.

128. *Id.* at 40. Notably, biotech companies are legally permitted to patent research that incorporates donated individual genetic material. *Id.* at 38.

129. Roberts, *supra* note 12, at 51.

130. *Id.* at 54. For example, indigenous groups with "uniquely appealing genetic profiles," whose genetic material was harvested for scientific research without compensation, complained they were subjected to a form of "molecular colonialism." Kara H. Ching, Note, *Indigenous Self-Determination in an Age of Genetic Patenting: Recognizing an Emerging Human Rights Norm*, 66 FORDHAM L. REV. 687, 697 (1997). Another example which has received a significant amount of public scrutiny is the sequencing and publishing of the genome of Henrietta Lacks, which occurred without her family's permission. Roberts, *supra* note 12, at 49.

131. Roberts, *supra* note 12, at 44. There is an argument that "the absence of ownership claims in genetic material—or more specifically excised cells—does not foreclose the possibility of an ownership claim in genetic information," as common law cases such as *Moore v. Regents of the*

These two warring principles encapsulate the bioethical dilemma inherent in the DTC-GT industry's use and sale of genetic data for medical research purposes.[132] Few would seek to impede research that can potentially improve or save lives with (ostensibly) little harm to the consumer. Indeed, some DTC-GT consumers consent to share their genetic data *because* they want to further a form of genetic research.[133] To legally recognize genetic data as a form of individual property could conceivably disturb this research process, perhaps by throwing the patentability of medical products influenced by DTC-GT consumer data into question, thereby weakening a major financial incentive for private research companies to pursue their work.[134] Nevertheless, as Professor Jessica Roberts notes, the industry's commodification and near-autonomous control of genetic data raises clear "non-economic, identity, and dignity-related concerns" which seemingly compel the need for a middle ground to be struck.[135]

2. The Wealth-Maximization Theory and the Case for Equitable Compensation

To help rectify this dilemma, Roberts argues that the central goal of genetic ownership law should be redefined as the maximization of social welfare.[136] This utilitarian framework broadly dictates that genetic ownership rights should be allocated on a case-by-case basis in the most socially beneficial manner—one that optimally recognizes the personal and economic interests at stake.[137] Of course, how social optimality is defined and evaluated remains subjective, enabling variations of the same personhood-labor theory debate to remain viable (though Roberts slightly narrows the inquiry by suggesting human happiness as a suitable barometer).[138]

Notwithstanding its lack of a bright-line rule, Roberts' framework offers the most appropriate set of parameters to tackle the issues facing the DTC-GT industry and its consumers. It acknowledges, for example, the consumer's limited bargaining power (e.g., her inability to control who her data can be shared with) as a strong

---

University of California only address tangible human material (i.e., spleen cells) and not the genetic information they contain. *Id.* at 46.

132. McFadden et al., *supra* note 1.

133. *Cf.* Roberts, *supra* note 12, at 44–45 (discussing genetic donors' altruistic motivations in the context of hospital-based research).

134. *Id.* at 40–41.

135. *Id.* at 52.

136. *Id.* at 63.

137. *Id.*

138. *Id.* at 59.

disincentive to would-be users and, thus, a constraining force on the pool of genetic data available for socially beneficial research.[139] Accordingly, to remedy this market defect, Roberts suggests improving the initial bargaining status of DTC-GT consumers by affording them "heightened rights in [their] genetic information."[140]

While workable in theory, even Roberts admits that the implementation of her framework on a case-by-case basis is limited in practicability.[141] A more realistic solution, however, may simply be one which allows genetic researchers to compensate DTC-GT consumers directly in exchange for their data.[142] This form of "equitable compensation"—while perhaps imperfect in its ability to fully address or offset the array of privacy concerns or dignitary injuries described in Part I—would certainly vindicate consumer interests at a higher level and continually incentivize individuals to contribute to genetic research.[143] It would also cut out the need for researchers to depend on DTC-GT firms as data intermediaries, insulating their research efforts from a potential drop in demand for a specific DTC-GT firm's services.

Such offerings, of course, are unheard of in the DTC-GT space.[144] The genetic sequencing industry, however, is a different story. Indeed, in explicit recognition of the social welfare dilemma described above, several sequencing start-ups have begun to offer equitable compensation models for their customers.[145] One model seeks to create a "genomic marketplace" that directly facilitates cryptocurrency transactions between researchers and consumers, who, through blockchain technology, may decide whether to rent or sell their data to an institutional suitor.[146] Another, using similar technology, rewards consumers who share their genetic data with company stock.[147]

These models, of course, are non-exhaustive; a DTC-GT firm that hypothetically chose to compensate its consumers could do so however it wished. The point remains—particularly in light of the escalation of lucrative DTC-GT industry partnerships—that major DTC-GT firms are capable of better incentivizing consumers to share

---

139. *Id.* at 60.

140. *Id.*

141. *Id.* at 63.

142. Grishin et al., *supra* note 14, at 6.

143. *Id.*

144. *See, e.g.*, *Individual Data Sharing Consent*, *supra* note 76 (declaring that consumers whose genetic data ultimately contributes to the development of "new commercial products or services . . . will not receive any compensation").

145. Grishin et al., *supra* note 14, at 4–5.

146. *Id.*

147. *Id.*

their personal data. However, as described in Part IV (and as one might expect), these firms have little desire to do so.

III. BLOCKCHAIN-BASED PLATFORMS AS A REMEDY

A. Blockchain: A Basic Primer

The common thread uniting nearly all of the genetic sequencing companies that have adopted equitable compensation models is their use of blockchain technology.[148] Blockchain technology is best known for facilitating the popular Bitcoin network, but it bears emphasis that it has an array of uses beyond the cryptocurrency sphere.[149] This Note focuses almost exclusively on blockchain's unique ability to grant consumers full and secure control over their genetic information (i.e., to determine who it is shared with and on what terms) when used in conjunction with smart contract technology. To understand how this is possible, however, it is necessary to first broadly (and simplistically) cover the technology's fundamentals. To be sure, this analysis is far from exhaustive; it only seeks to broadly acquaint the reader with certain characteristics of blockchain technology that are relevant to the privacy and bioethical concerns thus described.[150]

1. Decentralization

At a high level, blockchains are merely sophisticated data storage systems.[151] More commonly, they are defined as distributed or decentralized ledgers of information that are packaged together in bundles known as "blocks."[152] Each block is sequentially chained together and secured by an enhanced form of encryption known as

148. Grishin et al., *supra* note 14, at 5 (describing the compensation models of LunaDNA and EncrypGen—both of which incorporate blockchain technology—and diagramming the role of blockchain within Nebula's compensation model).

149. Ozercan et al., *supra* note 6, at 1256.

150. This Note does not cover, for example, the distinction between decentralized, distributed, and permissioned blockchains. It should be noted, however, that permissioned blockchains—which require access to be granted to each specific node—are accordingly more centralized in nature and, thus, are relatively more likely to suffer the same ills as normal, centralized networks. *See* Gwyneth Iredale, *Introduction to Permissioned Blockchains*, 101 BLOCKCHAINS (June 2, 2019), https://101blockchains.com/permissioned-blockchain [https://perma.cc/BL2Q-79YD].

151. PRIMAVERA DE FILIPPI & AARON WRIGHT, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 27 (2018).

152. Ozercan et al., *supra* note 6, at 1256.

"cryptographic hashing."[153] Blockchains are not stored in any one place (such as a cloud-based server) or controlled by a single entity.[154] Rather, a copy of each chain is stored in its entirety on a series of "nodes" (for example, the computer of someone connected to the blockchain network) that are in constant communication with one another, and that, crucially, must come to a consensus that *any* proposed alteration of a block is valid.[155] Because each node operates independently from one another, no single point of attacking a network exists.[156] Thus, the decentralized consensus mechanism—in conjunction with the high-strength encryption of each block—effectively shields information stored on a blockchain from unauthorized access.[157]

2. Mining

Each block is imbued with a "unique fingerprint" of code (known as a "hash"), a time stamp, and the hash of the block preceding it.[158] The process of generating a new block is referred to as "proof of work," which requires certain users (known as "miners") to solve a complex mathematical problem that verifies both the information contained within the block and its respective hash.[159] The rigorous nature of this process is intended to make altering the information stored on the blockchain exceptionally difficult, thereby securing network integrity.[160] Indeed, it would be prohibitively expensive for any private party to attempt to manipulate the blocks stored on a major protocol such as Bitcoin.[161]

---

153. *Id.* ("Cryptographic hashes are summaries of data in binary format in which one small change in the original data yield a 50% chance of changing every bit of the earlier hash value. This means that it is impossible to find data that corresponds to a desired hash value due to its highly probabilistic and volatile nature.").

154. *Id.*

155. DE FILIPPI & WRIGHT, *supra* note 151, at 2; Jimi S., *Blockchain: What Are Nodes and Masternodes?*, MEDIUM (Sept. 5, 2018), https://medium.com/coinmonks/blockchain-what-is-a-node-or-masternode-and-what-does-it-do-4d9a4200938f [https://perma.cc/PHG6-JXY5].

156. DE FILIPPI & WRIGHT, *supra* note 151, at 2.

157. *Id.*

158. *Id.* at 22.

159. *Id.* at 23.

160. *Id.*

161. One example of said manipulation is a "51% attack," whereby a single organization or entity amasses enough mining power within a single network to effectively control and modify transactions. *Id.* at 25. Directing such an attack on a major network such as Bitcoin (which has thousands of nodes) would cost "hundreds of millions of dollars, if not billions." *Id.* Even if such an attack were to occur, it would *only* risk the alteration of blocks generated during the period in which the attackers have control—that is, blocks that existed before the attack occurred would still remain virtually impenetrable. Jake Frankenfield, *51% Attack*, INVESTOPEDIA,

3. Diagramming Blockchains by Analogy

Analogizing these components to a digestible scenario may be helpful to better understand both their function and usefulness in the DTC-GT context.[162] One such analogy posited by Professor Halil Ozercan first asks the reader to envision a town where all the banks have failed due to a repetitive spurt of government corruption.[163] After the townspeople collectively decide that their reliance on centralized banks to store their financial information is no longer viable, a solution is formed[164]:

> [First, a] town meeting is called, and everyone joins with a new notebook. All citizens report and prove how much money they own. Everyone takes note of each other. After the meeting, when someone makes a transaction for any reason, they must announce this to everyone they know. If someone hears about a transaction, they make a note of [it on] the ongoing page of their notebook. They also must pass the information until it eventually reaches all townspeople. [Once this occurs,] [t]he transaction is considered to be completed, and accounts are updated when the page that contains it is closed. Everyone must close an ongoing page roughly at the same time. To achieve this . . . scientists of the town proposed a self-updating puzzle. When someone solves this puzzle, they publish their result with their ongoing page. If the solution is correct and their ongoing page does not include a faulty transaction, everyone copies the given page and closes it after adding a "rewarding transaction" (i.e., new "money") to the solver.[165]

The citizens in this example represent the "nodes" which foster the blockchain infrastructure, while their notebooks embody each node's continually updating copy of the blockchain. Each page within that notebook and the personal financial information written upon it embodies a block.[166] The fact that each page must be closed at the same time (the consensus mechanism) in conjunction with the solution of a complex puzzle (the mining process, known as "proof of work") is a testament to the integrity and security of information stored on the blockchain; unless each citizen is on the same page, so to speak, the existing chain of information will go unaltered.[167]

---

https://www.investopedia.com/terms/1/51-attack.asp [https://perma.cc/79HW-ACXT] (May 6, 2019).

162. *See* Ozercan et al., *supra* note 6, at 1258.

163. *Id.*

164. *Id.*

165. *Id.*

166. *Id.*

167. *Id.*

B. The Utility of Smart Contracts and the Rise of "Blockchain Genomics"

1. What Are Smart Contracts?

Blockchains, as data storage systems, are able to retain or reference a variety of information, including a form of computer program colloquially known as a "smart contract."[168] For the purposes of this Note, smart contracts can be thought of as an autonomous, tamper-proof escrow accounts,[169] or, more specifically, as automated, self-executing digital agreements that are dependent on blockchain technology.[170] The basic concept of a smart contract is simple: once a party fulfills its performance obligations—memorialized via program code and embedded within a blockchain network—the other party is automatically compelled to execute its side of the deal.[171] This means that when both parties agree to exchange purely digital information (as in the online purchase of an individual's genetic information), the need for any intermediary or operator to enforce the contract's terms disappears.[172]

By ensuring mutual performance, smart contracts can operate as a critical tool in the equitable compensation movement, allowing consumers and firms to structure an array of flexible transactions. Anyone who possesses their own genetic data could, for example, "rent" it to a research entity via smart contract with the trust that the program will (i) ensure they get paid and (ii) automatically prohibit access to their data once the rental period expires.[173]

2. Use Case: Nebula Genomics

Smart contract technology is already being used to grant genetic-testing consumers the ability to rent or sell their information on

168. DE FILIPPI & WRIGHT, *supra* note 151, at 27.

169. Deryck Gebe, *How Smart Contracts and Stablecoins Will Reshape Escrow*, CRPYTOSLATE (July 3, 2018, 2:00 PM), https://cryptoslate.com/how-smart-contracts-and-stable-coins-will-reshape-escrow/ [https://perma.cc/3WBM-ZAVG].

170. *See* DE FILIPPI & WRIGHT, *supra* note 151, at 74 ("Smart contract code is executed in a distributed manner by all of the nodes supporting the underlying blockchain-based network, without necessarily relying on any intermediary operator or trusted middleman.").

171. *Id.*

172. *Id.*

173. Ozercan et al., *supra* note 6, at 1261.

their own (relative) terms.[174] Perhaps the best example of this system is the blockchain-based network engineered by Nebula Genomics, a direct-to-consumer sequencing firm that seeks to facilitate genetic research by giving consumers the ability to own and control access to their data.[175] In line with this objective, the Nebula network provides a secure marketplace for "data buyers" (i.e., genetic researchers) and "data owners" (i.e., Nebula customers, or customers of other genetic testing firms) to negotiate and execute genetic data transactions through customized smart contracts.[176]

First, to find the data they need, researchers may query the network for the results of optional health surveys filled out by anonymous data owners before or after their genetic samples are sequenced.[177] Once the buyer identifies a subject for research, they may create a smart contract that specifies both the blockchain address of the data's respective owner (who remains anonymous) and bid for their data, or, if they have yet to be sequenced, subsidize their sequencing costs.[178] The owner may thereafter accept or reject the contract's terms, perhaps because the bid is too low, or because they are repulsed by the identity of the research institution soliciting their data.[179] If the offer is accepted, the proposed smart contract is executed, resulting in the simultaneous exchange of Nebula tokens and access to the owner's data.[180] The terms of the buyer's access are subsequently registered on the blockchain and enforced by the network's system of nodes.[181]

---

174. *See, e.g.*, *id.* (describing the use of smart contracts in Nebula's business model and that of Zenome, which similarly allows users to sell their genetic information).

175. *See* DENNIS GRISHIN, KAMAL OBBAD, PRESTON ESTEP, MIRZA CIFRIC, YINING ZHAO & GEORGE CHURCH, NEBULA GENOMICS: BLOCKCHAIN-ENABLED GENOMIC DATA SHARING AND ANALYSIS PLATFORM 23 (2018), http://arep.med.harvard.edu/pdf/Grishin_Church_v4.52_2018.pdf [https://perma.cc/2VVL-H9NS]. The Nebula network is specifically built on Blockstack, a decentralized computing platform used for storage purposes, and the Ethereum-based Nebula blockchain. *Id.* at 15, 18.

176. Grishin et al., *supra* note 14, at 11. Nebula ensures consumers that "multiple mechanisms" are used to safeguard their genomic data and other personal information. GRISHIN ET AL., *supra* note 175, at 12. These mechanisms largely consist of allowing users to privately store and regulate access to their data via Blockstack, protecting their data and survey responses using homomorphic encryption, and storing all transaction records (but not genomic data) on the Nebula blockchain. *Id.* at 12, 15–18.

177. *Id.* at 18–19.

178. *Id.* at 23.

179. Grishin et al., *supra* note 14, at 18.

180. *Id.*; GRISHIN ET AL., *supra* note 175, at 23.

181. Grishin et al., *supra* note 14, at 18.

3. Important Limitations of Blockchain-Based Genomic Networks

By granting users the power to broker their own genetic data on a secure and transparent system, the Nebula network represents both the antithesis of modern DTC-GT data-sharing practices and, as of now, the most socially optimal method of facilitating genetic research. Notwithstanding its comparative benefits, however, the concept of a blockchain-based genomic marketplace itself carries its own set of consumer-facing issues (albeit ones that are seemingly more manageable relative to those associated with the DTC-GT industry). Chief among these is the immutability of the blockchain, which effectively prevents parties who enter into a smart contract from being able to alter its terms or back out of a transaction.[182]

With regard to Nebula specifically, it also remains unclear whether data that is transacted for can be exfiltrated from the system by whoever purchases it.[183] Moreover, because it is infeasible (given its size) to store an individual's fully sequenced genome on the blockchain, the genetic data itself must remain off-chain.[184] This would diminish the strength of the Nebula network's security. To its credit, Nebula thinly addresses this concern by giving consumers the flexibility to choose how their data is privately stored.[185] It fails to remedy, however, the fact that the actual sequencing of genetic samples must flow through its own servers, adding a degree of centralization that brings with it the same aforementioned risks of genetic exposure.[186] This dilemma, however, could only be avoided by decentralizing the sequencing process—that is, by enabling individuals to sequence themselves.[187] This would require portable sequencing machines, which remain mere "hypothetical proposal[s]" within the genomics community.[188]

Nebula's compensation system also raises its own ethical concerns. For one, data owners are only able to receive compensation by either having the costs of sequencing subsidized by a data buyer[189]

182. *Id.* at 8.

183. Brad Jones, *Nebula Genomics Will Let You Rent Out Your Genetic Information*, FUTURISM (Feb. 20, 2018), https://futurism.com/nebula-genomics-rent-genetic-information [https://perma.cc/4AN8-LKUB].

184. Ozercan et al., *supra* note 6, at 1261–62.

185. GRISHIN ET AL., *supra* note 175, at 18.

186. *Id.* at 24.

187. *Id.*; Ozercan et al., *supra* note 6, at 1262.

188. Ozercan et al., *supra* note 6, at 1262.

189. GRISHIN ET AL., *supra* note 175, at 23. It remains unclear whether or not Nebula has actually implemented this subsidy option for consumers. *See* NEBULA GENOMICS, *FAQ*,

or, if they've already paid for sequencing services, exchanging their genetic data for Nebula tokens (sold by Nebula to data buyers for fiat money) that are only redeemable for additional Nebula-related services.[190] It is fair to question whether this practice truly represents an equitable form of compensation. Moreover, even if Nebula permitted data owners to monetarily benefit from their sequenced data, they may not understand its true fair market value, allowing researchers to purchase it for a price far below its true worth.[191]

In spite of these concerns, blockchain-based networks like Nebula's offer an intriguing pathway forward for the genetic testing industry as a whole. No other form of data management is simultaneously capable of addressing the previously noted bioethical concerns while also ensuring the flow of genetic information for beneficial research. Consumer advocates should thus take heart in the fact that such genomic marketplaces are slightly on the rise: other start-ups, like EncrypGen or Zenome, either currently or plan to offer researchers the opportunity to purchase genetic data directly from consumers in exchange for cryptocurrency.[192] However, unlike Nebula, neither of these firms seem to offer in-house sequencing services[193] and, in the case of EncrypGen, are relatively less transparent with how their blockchain systems work.[194] Thus, as of now, the Nebula model seems to be the gold standard—one that major DTC-GT firms might do well to study and potentially emulate in the near future.

IV. THE FTC AS A FACILITATIVE VEHICLE FOR BLOCKCHAIN ADOPTION

A. When Market Forces Won't Work: A Space for Limited Regulatory Action

To some degree, the public's increasingly skeptical approach to both the security of genetic data and the ethics of its sale likely

https://nebulagenomics.zendesk.com/hc/en-us/sections/360003713751-FAQ (last visited Feb. 6, 2020) (failing to mention any form of available consumer subsidy).

190. GRISHIN ET AL., *supra* note 175, at 14.

191. *See* Grishin et al., *supra* note 14, at 19 ("Personal data marketplaces also would be asymmetric, since individuals are likely to be unaware of the value of their personal data and are thus at risk of not being compensated fairly.").

192. Ozercan et al., *supra* note 6, at 1261; *Our Views & Directions*, ZENOME, https://zenome.io/about/ [https://perma.cc/B9CG-44TC] (last visited on Feb. 6, 2020).

193. Ozercan et al., *supra* note 6, at 1261; *see* Emily Mullin, *This New Company Wants to Sequence Your Genome and Let You Share It on a Blockchain*, MIT TECH. REV. (Feb. 7, 2018), https://www.technologyreview.com/2018/02/07/145768/this-new-company-wants-to-sequence-your-genome-and-let-you-share-it-on-a-blockchain/ [https://perma.cc/PS2A-6TKS].

194. Ozercan et al., *supra* note 6, at 1261.

contributed to the DTC-GT industry's recent slump.[195] Nevertheless, industry-leading firms—which, as discussed, have a vested interest in controlling consumer information—seem more willing to speculate other, broader economic trends as a cause of slowed sales.[196] Assuming, however, the aforementioned concerns are at least partially to blame for the industry's rut, it would illuminate a financial incentive for DTC-GT firms to embrace more transparent, secure, and equitable data management practices.

Perhaps, then, the DTC-GT market will adjust on its own. One could assume that as the Nebulas of the world grow in number and legitimacy, so too will their customer bases, creating further pressure for DTC-GT firms to offer analogous, consumer-friendly features (e.g., heightened security and compensation) or even adopt blockchain-based platforms. Leaving the market to its own devices, however, is unlikely to produce any noticeable shift in firm behavior. For one, larger firms like 23andMe and Ancestry enjoy massive user bases, resources, and brand recognition which affords them a sizable "first mover advantage" over smaller competitors.[197] This grants them the institutional legitimacy needed to secure special FDA clearance to market predictive health tests—potentially a substantial hurdle for younger firms—and the financial security to explore new ways of generating revenue.[198] 23andMe, for instance, recently sold the rights to a drug it developed in-house, the first of many licensing deals in its future.[199] All told, it seems unlikely that larger DTC-GT firms will face any formidable market pressure to change the way they store and use genetic information; absent an external force, DTC-GT firms will continue to monetize—not undermine—their ability to control it.

---

195. *Has the Consumer DNA Test Boom Gone Bust?*, ADVISORY BD. (Feb. 20, 2020), https://www.advisory.com/daily-briefing/2020/02/20/dna-tests [https://perma.cc/H24J-K7RG] [hereinafter ADVISORY BD.].

196. *See* Roberts, *supra* note 33 ("[23andMe's CEO] acknowledges 'privacy is top of mind' for consumers right now, but she also theorizes the problem could be fears of a recession.").

197. Evan Tarver, *First Mover Definition*, INVESTOPEDIA, https://www.investopedia.com/terms/f/firstmover.asp [https://perma.cc/V45H-FB5V] (Sept. 28, 2020); *see* Regalado, *supra* note 1 (describing the size and reach of larger DTC-GT firms). This market advantage is solidified by a "network effect": the "more individuals join a database, the more useful it is for finding relatives, for creating ancestry estimates, and (in the case of 23andMe) as a basis for drug research." *Id.*

198. *See* Clayton et al., supra note 11, at 16 (describing 23andMe's passage through various FDA hurdles to market predictive health tests).

199. Nicole Wetsman, *23andMe Sold the Rights to a Drug It Developed from Its Genetic Database*, THE VERGE (Jan. 10, 2020, 3:50 PM), https://www.theverge.com/2020/1/10/21060456/23andme-licensed-drug-developed-genetic-database-autoimmune-psoriasis-almirall.

B. Using the FTC's "Information-Forcing" Tools to Study and Encourage Blockchain Adoption

1. Why the FTC?

From a social welfare perspective, *some* form of intervention into DTC-GT data-management practices seems appropriate—particularly one that promotes the broader adoption of blockchain technology by DTC-GT firms.[200] This could take a variety of forms. Congress, of course, could finally address genetic privacy issues by enacting legislation that mandates DTC-GT firms to adopt more secure and transparent data-management practices, similar to the state laws of Alaska or Nevada.[201] Alternatively, regulators like the FTC could attempt to shoehorn in those practices through rulemaking or adjudicative enforcement.[202] However, as discussed below, such aggressive tactics are inadvisable given their potential to economically disrupt DTC-GT firms or discourage them from developing innovative, consumer-friendly platforms.[203]

Notably, those who advocate for enhanced regulatory oversight of the DTC-GT industry frequently cite the FTC as the appropriate body to spearhead the effort.[204] Indeed, the FTC, which carries the broad statutory authority to police "unfair or deceptive" commercial practices,[205] now resonates as "the closest thing the United States has to a privacy regulator,"[206] overseeing or engaging in privacy-oriented "civil law enforcement, business outreach and consumer education,

200. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 175 (2016) (remarking that, in self-regulating industries, "some external force, such as threat of suit from the government or legislation," can cause industries to effectively regulate themselves in the public interest).

201. *Supra* Section I.D.2.

202. *Infra* Section IV.B.

203. Walter G. Johnson, *Blockchain Meets Genomics: Governance Considerations for Promoting Food Safety and Public Health*, 15. J. FOOD L. & POL'Y 74, 94 (2019).

204. This includes Senate Minority Leader Chuck Schumer, who, in 2017, "convened a press conference to warn consumers of the potential risks of at-home DNA testing" and "asked the [FTC] 'to take a serious look at this relatively new kind of service and ensure that these companies have clear, fair privacy policies and standards for all kinds of at-home DNA test kits.'" Hazel & Slobogin, *supra* note 20, at 36–37.

205. Federal Trade Commission Act, Pub. L. No. 63-203, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. §§ 41–58).

206. Kate Cox, *FTC Head Asks Congress for Real Privacy Laws He Can Enforce*, ARS TECHNICA (Nov. 14, 2019, 2:07 PM), https://arstechnica.com/tech-policy/2019/11/we-need-help-from-you-on-creating-privacy-law-ftc-chair-tells-congress/ [https://perma.cc/TF8U-KUJE].

policy initiatives, and recommendations to Congress to enact legislation" for more than a decade.[207]

Notwithstanding its broad scope of authority, the FTC reserves its enforcement power solely for those businesses that either deceive consumers regarding their level of privacy or fail to implement "reasonable" data security measures,[208] an objective standard that weighs various consumer- and business-facing interests against one another.[209] Enforcement actions of either variety, while growing in frequency, are usually rare, and normally (but not always) occur in the aftermath of a large-scale data breach or severe mishandling of consumer information.[210] As the FTC lacks injunctive authority, it often seeks to enter into rigid, court-enforced settlement agreements known as "consent orders" that bind the target business to pay a certain civil penalty and adopt enhanced privacy or security practices.[211] Because the FTC publishes its consent orders, they also result in steep negative publicity for the business.[212]

In 2018, the FTC made a de facto public admission regarding the launch of an investigation into the general privacy policies of DTC-GT firms.[213] The status of this inquiry is unknown, though it bears noting that the FTC's investigations are incredibly lengthy, often taking more

---

207. Andrea Arias, *The NIST Cybersecurity Framework and the FTC*, U.S. FED. TRADE COMM'N: BUS. BLOG (Aug. 31, 2016, 2:34 PM), https://www.ftc.gov/news-events/blogs/business-blog/2016/08/nist-cybersecurity-framework-ftc [https://perma.cc/WG2X-XBPY].

208. HOOFNAGLE, *supra* note 200, at 123; Arias, *supra* note 207. Notably, the FTC defines "deception" to involve, inter alia, "a representation, omission, or practice that is likely to mislead a consumer." HOOFNAGLE, *supra*. This entails the FTC to evaluate, from the consumer's perspective, "the clarity of the representation," whether the target business "qualifies the representation," and the importance of the omitted information. *Id.* at 125.

209. Specifically, the FTC weighs whether the company's data security measures are "reasonable in light of the volume and sensitivity of information the company holds, the size and complexity of the company's operations, the cost of the tools that are available to address vulnerabilities, and other factors." Arias, *supra* note 207.

210. The FTC has settled over sixty data security cases since 2001, seven of which came in 2019. Arias, *supra* note 207; Andrew Smith, *New and Improved FTC Data Security Orders: Better Guidance for Companies, Better Protection for Consumers*, U.S. FED. TRADE COMM'N: BUS. BLOG (Jan. 6, 2020, 9:46 AM), https://www.ftc.gov/news-events/blogs/business-blog/2020/01/new-improved-ftc-data-security-orders-better-guidance [https://perma.cc/DZ49-4Q4V].

211. HOOFNAGLE, *supra* note 200, at 113–16.

212. *See, e.g.*, *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*, U.S. FED. TRADE COMM'N (July 22, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related [https://perma.cc/L2KX-L374].

213. Baram, *supra* note 92.

than a year to complete.[214] Thus, it is possible that a major DTC-GT player could soon be the target of an enforcement action. Nevertheless, if the goal is to promote a more socially optimal genetic testing industry, targeted enforcement would likely prove counterproductive. A widely publicized consent order, for instance, could compound already shaky consumer confidence in genetic testing, further diminishing test kit sales and, thus, the pool of information available for publicly beneficial research.[215] This would neutralize a significant rationale for implementing the technology in the first place.[216] Moreover, it may lock certain businesses into adopting a security or privacy practice (e.g., a type of encryption) that may soon be obsolete.

Recognizing the significance of its enforcement power, the FTC primarily relies on softer, "information-forcing" methods to initially encourage businesses to adopt better privacy practices.[217] This usually involves (i) sponsoring industry-specific "workshops," a public forum that brings together stakeholders to discuss "privacy problems, new business models, and public policy approaches;"[218] (ii) publishing guidance;[219] and (iii) endorsing voluntary standards crafted by nonregulatory agencies, as it recently did with the National Institute of Science and Technology's (NIST) Cybersecurity Framework.[220] All of these methods suffice as a way for the FTC to both build proper expertise and signal its preference for a specific practice or behavior *without* exercising its legal authority—potentially inducing risk-averse businesses into preemptive compliance.[221]

---

214. Christopher Soghoian, *How Long Does It Take for the FTC to Investigate a Company?*, SLIGHT PARANOIA (Feb. 8, 2012), http://paranoia.dubfire.net/2012/02/how-long-does-it-take-for-ftc-to.html [https://perma.cc/UJ5X-3DAA].

215. *See* ADVISORY BD., *supra* note 195 (discussing the role of privacy concerns in the industry's sales slump); *see also supra* Section III.B (discussing blockchain technology's ability to benefit researchers by cutting out DTC-GT middlemen and incentivizing consumers to participate in genetic testing).

216. *See* McFadden et al., *supra* note 1.

217. HOOFNAGLE, *supra* note 200, at 158 ("Procedurally . . . the FTC enters new areas of [privacy] law [in a certain manner]: First come warnings in the form of letters, workshops, and other public pronouncements. Shortly thereafter, the FTC brings matters against particularly egregious transgressors.").

218. *Id.* at 100.

219. Arias, *supra* note 207.

220. *Id.*

221. *See* HOOFNAGLE, *supra* note 200, at 121 (remarking how the FTC's informational tools often allow counsel for businesses to "read the FTC's many tea leaves" before it engages in targeted enforcement).

2. Proposal: Forming a "Blockchain Genomics" Task Force for Consumer Education and Voluntary Standard Promulgation

The FTC can and should rely on information-forcing practices to encourage the adoption of blockchain-based platforms in the DTC-GT industry. Ideally, this would entail the publication of agency guidance that better informs consumers of the risks of genetic exposure, gives risk-averse DTC-GT firms the chance to prudently adjust their information management systems, and provides the basis for future enforcement actions.

While this process could take a variety of forms, it should broadly consist of at least two stages—namely, a period of agency and stakeholder education followed by the endorsement or publication of voluntary standards.

First, to grasp how blockchain technology can assist the responsible management of genetic data, the FTC should task its own "Blockchain Working Group" (launched in 2018 to study fraudulent cryptocurrency activity), to conduct market research.[222] This should include a comprehensive study of the DTC-GT industry's information management practices, assessment of blockchain technology's evolving uses and functionality, and a general evaluation of its strengths and weaknesses in reducing consumer privacy risks. The Working Group should also establish collaborative channels with research agencies like NIST (which has already published a general blockchain study) to fill in any technical knowledge gaps.[223] The information gleaned from this stage could then be distilled into digestible pieces of agency guidance made available to the public. It could also spur informative dialogue between the FTC and industry stakeholders at future agency-sponsored "workshops."[224]

Next, the FTC should publish voluntary standards that encourage DTC-GT firms to integrate blockchain technology with their information management systems.[225] These standards could, for example, be the basis for an incentive system analogous to the Center for Medicaid Service's (CMS) Electronic Health Record (EHR) Incentive Program, which "provide[s] incentive payments to eligible . . . hospitals

---

222. Neil Chilson, *It's Time for a FTC Blockchain Working Group*, U.S. FED. TRADE COMM'N: TECH@FTC BLOG (Mar. 16, 2018, 11:29 AM), https://www.ftc.gov/news-events/blogs/tech-ftc/2018/03/its-time-ftc-blockchain-working-group [https://perma.cc/MW7F-GFMS].

223. *See* DYLAN YAGA, PETER MELL, NIK ROBY & KAREN SCARFONE, NAT'L INST. STANDARDS & TECH., BLOCKCHAIN TECHNOLOGY OVERVIEW (2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf [https://perma.cc/79FF-FMCZ].

224. HOOFNAGLE, *supra* note 200, at 100.

225. Johnson, *supra* note 203, at 96.

as they demonstrate adoption, implementation, upgrading, or meaningful use of certified EHR technology."[226] Alternatively, the FTC could merely suggest that preemptive compliance with these standards will likely insulate a DTC-GT from a future enforcement action. To determine the best course of action, the agency could once again rely on the outside expertise of NIST—which regularly revises EHR Incentive Program standards—or a private standard-setting body like the ISO or Institute of Electrical and Electronics Engineers (IEEE).[227]

Notably, both stages of the standard-setting process would require the FTC to confront several thorny policy issues. Principally, the agency would need to determine a type of blockchain ledger to endorse (e.g., permissioned or permission-less, a distinction that this Note, for purpose of brevity, does not cover); how genetic data should be valued; and how much control individuals should maintain over their data throughout a given transaction. Overall, the FTC would need to determine just how far it should go to spur DTC-GT firms to adopt blockchain technology—ultimately requiring the agency to weigh the private costs of blockchain adoption against the public costs of allowing DTC-GT firms to broker their customers' genetic data.

V. CONCLUSION

The ability for DTC-GT firms to centralize and subsequently peddle the genetic information of consenting consumers raises serious privacy and bioethical concerns. In the absence of substantive regulatory oversight, these consumers place themselves at risk of genetic exposure—which, for them or their family, could prove devastating, particularly as DNA is increasingly used to identify individuals and secure their possessions. They also open themselves up to the wider dignitary harm of having fundamentally defining information used for profit without compensation. Ironically, these concerns may ultimately constrain the overall pool of genetic information available for beneficial medicinal research by disincentivizing consumers from taking a genetic test in the first place.

As start-ups like Nebula demonstrate, the adoption of blockchain technology within the genetic testing industry presents a feasible way to help remedy some or all of these concerns. Yet, in the absence of serious competition, major DTC-GT firms have little incentive to explore these systems. There is, however, ample room for a

226. *Promoting Interoperability Programs Registration System*, CTR. FOR MEDICAID SERVS., https://ehrincentives.cms.gov/hitech/loginCredentials.action [https://perma.cc/ZRP6-D3RC] (last visited Jan. 28, 2021).

227. Johnson, *supra* note 203, at 96.

privacy regulator like the FTC to wield its soft power to nudge the industry in that direction, laying a foundation for its widespread adoption of blockchain technology in the not-so-distant future.

Noah Spector[*]

[*] J.D. Candidate, Vanderbilt University Law School, 2021; B.A., The Ohio State University, 2018. The author would like to thank his grandparents, Fred and Buzzy; parents, Leslie and David; and siblings, Sam, Ian, Alex, Or, Sarah, and Ryan for their constant love and support. The author would also like to thank his baby niece, Eden, who brought happiness and joy to a year where it was needed the most. Finally, thanks are in order for the *Vanderbilt Journal of Entertainment and Technology Law* staff, whose helpful insight and edits greatly facilitated the publication of this Note.