Genetic Data Privacy Solutions in the GDPR

Kristi Harbord

Texas A&M University School of Law (Student), kharb1790@tamu.edu

Recommended Citation

COMMENT

GENETIC DATA PRIVACY SOLUTIONS IN THE GDPR

By: Kristi Harbord*

ABSTRACT

The intersection of healthcare and technology is a rapidly growing area. One thriving field at this intersection involves obtaining, processing, and storing genetic data. While the benefits have been great, genetic information can reveal a great deal about individuals and their families. And the information that can be conveyed from genetic data appears limitless and is constantly growing and changing. Many entities have begun storing, processing, and sharing genetic data on a very large scale. This creates many privacy concerns that the current regulatory framework does not account for. The line between patient data and consumer data is blurred; many entities are interested in obtaining genetic data with varied interests. In the direct-to-consumer genetic testing market, consumers pay to send private companies their DNA samples in exchange for a trivial amount of information about their ancestry and health risks. But health data obtained and processed by a company are subjected to far less stringent privacy regulations than health data obtained and processed at a doctor's office or hospital. This Comment summarizes some of the current genetic privacy problems in United States laws and examines the EU's recently adopted GDPR for a possible solution. A GDPR-style regulation could provide more consistency, give individuals more control, and protect against future unknown uses.

TABLE OF CONTENTS

I. Introduction

Healthcare has entered the "age of genomics" with emerging technologies, big data, and complex analytics driving rapid advancements in genomic research.[1] This research requires access to immense stores of individual genetic and associated health data.[2] In September 2018, the National Institutes of Health ("NIH") provided $28.6 million in funding to establish three large-scale genome centers, focused on generating genomic data.[3] The participants in this program will share their genetic information and health records.[4] In return, participants may receive information about their risk for diseases, drug-gene interactions, and ancestry information.[5] In addition, NIH awarded a $7 million contract to a software company that builds big-data platforms.[6] Scientists will use the new software and data platform with a goal to "accelerate the discovery of new therapies for cancer and other illnesses."[7] Ultimately, NIH hopes to create a database of more than one million biosamples and associated health information.[8]

Private companies are also collecting, storing, and sharing consumer health data on very large scales.[9] One example of massive genetic data collection by a private company is through direct-to-consumer DNA testing.[10] Direct-to-consumer DNA testing companies are growing

---

1. Fida K. Dankar et al., *The Development of Large-Scale De-Identified Biomedical Databases in the Age of Genomics—Principles and Challenges*, 12 Hum. Genomics 19, 1 (2018).

2. *Id.*

3. *NIH-Funded Genome Centers to Accelerate Precision Medicine Discoveries*, Nat'l Insts. Health (Sept. 25, 2018), https://allofus.nih.gov/news-events-and-media/announcements/nih-funded-genome-centers-accelerate-precision-medicine-discoveries [https://perma.cc/8UA9-N6FY].

4. *Id.*

5. *Id.*

6. *National Institutes of Health Awards Palantir with Contract to Advance Critical Health Research*, Bus. Wire (Sept. 21, 2018, 8:00 AM EDT), https://www.businesswire.com/news/home/20180921005056/en/National-Institutes-Health-Awards%20Palantir-Contract-Advance%20Critical%20Health%20Research [https://perma.cc/M3G2-6PYZ].

7. *Id.*

8. Nat'l Insts. Health, *supra* note 3.

9. *See* BIS Research, *Global Big Data in Healthcare Market to Reach $68.75 Billion by 2025, Reports BIS Research*, PR Newswire (Mar. 28, 2018, 7:30 AM ET), https://www.prnewswire.com/news-releases/global-big-data-in-healthcare-market-to-reach-6875-billion-by-2025-reports-bis-research-678151823.html [https://perma.cc/57EP-FLHT] (predicting that global big data in the healthcare market will reach $68.75 billion by 2025).

10. Tobias Haeusermann et al., *Open Sharing of Genomic Data: Who Does it and Why?* PLoS One, 2017, at 4.

rapidly and hiring new employees for "large-scale processing of genetics data."[11] For example, GlaxoSmithKline, one of the world's largest pharmaceutical companies, recently purchased a $300 million stake in 23andMe, a large private consumer genetic testing company.[12] Just months later, the FDA approved 23andMe's application to market reports regarding whether consumers may have genetic variants that could affect their reaction to certain medications.[13] Even Facebook tried to break into this field by attempting to partner with a hospital to combine patient information with social network information.[14]

The collection, storage, and sharing of massive amounts of genetic data by public and private entities raise many privacy concerns. First, the blurred line between public and private researchers, companies, patients, consumers, and hospitals means it can be difficult to know whom patients and consumers are sharing their information with and who is really benefitting. To blur the line further, companies have begun to partner with physicians to help customers interpret their results.[15] "Companies like Color Genomics and Invitae . . . allow consumers to order a genetic test through a physician or genetic counselor, who can help the customer interpret the results remotely."[16] Consumers are likely confused about who ultimately has access to their genetic data.

Second, scholars have concluded there are gaps in the current privacy and discrimination regulations.[17] Our current regulations offer far less protection for genetic data disclosed and processed by a private company as compared to disclosures of genetic data by a physi-

---

11. Jessica Kim Cohen, *23andMe is Hiring—Three Suggestions about the Company's Growth*, BECKER'S HEALTH IT & CIO REP. (Sept. 10, 2018), https://www.beckershospitalreview.com/data-analytics-precision-medicine/23andme-is-hiring-3-suggestions-about-the-company-s-growth.html [https://perma.cc/3J88-WZHC].

12. Jaime Ducharme, *A Major Drug Company Now Has Access to 23andMe's Genetic Data. Should You Be Concerned?*, TIME (July 26, 2018), http://time.com/5349896/23andme-glaxo-smith-kline/ [https://perma.cc/BS7U-KMQN].

13. Jessica Kim Cohen, *23andMe Moves Into Pharmacogenetics as FDA Greenlights New Test*, BECKER'S HOSP. REV. (Nov. 1, 2018), https://www.beckershospitalreview.com/supply-chain/23andme-moves-into-pharmacogenetics-as-fda-greenlights-new-test.html?origin=cioe&utm_source=cioe [https://perma.cc/7HLF-5AMY].

14. Kalev Leetaru, *Facebook's Medical Research Project Shows it Just Doesn't Understand Consent*, FORBES (Apr. 5, 2018, 11:36 PM), https://www.forbes.com/sites/kalevleetaru/2018/04/05/facebooks-medical-research-project-shows-it-just-doesnt-understand-consent/#555e6403453a [https://perma.cc/G6D9-DTWC].

15. Jessica Kim Cohen, *New 'Hybrid' Approach to DNA Testing Mixes Direct-to-Consumer, Clinical Care Models: 4 Notes*, BECKER'S CLINICAL LEADERSHIP & INFECTION CONTROL (Jan. 15, 2019), https://www.beckershospitalreview.com/quality/new-hybrid-approach-to-dna-testing-mixes-direct-to-consumer-clinical-care-models-4-notes.html [https://perma.cc/TZ7X-BK7Z].

16. *Id.*

17. Katherine Drabiak, *Caveat Emptor: How the Intersection of Big Data and Consumer Genomics Exponentially Increases Informational Privacy Risks*, 27 HEALTH MATRIX 143, 167 (2017).

cian or hospital.[18] Also, some have suggested that genetic data most likely cannot be anonymized.[19] If genetic data cannot truly be anonymous, then statutes that allow sharing "anonymized genetic data" are ineffective.[20] Additionally, genetic data can implicate family members who did not voluntarily provide their genetic data.[21] Regulations that require companies to obtain consent before sharing genetic data are not effective if an implicated family member never consented to share their information.[22] Government use of this data to implicate family members in the criminal law context is also a continuing concern.[23]

Finally, perfect compliance with all of the existing regulations is extremely difficult, if not impossible. Health research and reports were once mostly governed by hospitals and doctors' offices and subjected to laws that protected patient privacy.[24] But now these projects are frequently commercial private ventures subject to different laws.[25] Further, regulations relevant to genetic privacy are complex. State regulations vary in the degree of protection offered.[26] The federal and state regulations apply in different ways depending on how the information is obtained, where it is processed, where the customer lives, or where they obtain treatment.[27] It is often unclear which law or rule applies for each particular use.

This Comment argues that patient and consumer genetic data need more protection. The ideal solution would have strong privacy protection, clarity between states and sectors, and adaptability for the future.[28] This Comment argues that the United States should adopt a data privacy regulation similar to the European Union ("EU") framework, the General Data Protection Regulation ("GDPR"). Section II discusses what genetic big data is, its importance, and its unique po-

---

18. *Compare* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996), *with* 15 U.S.C. § 45(n) (2012).

19. *See* Drabiak, *supra* note 17, at 165.

20. *See id.*

21. *See id.* at 182.

22. *See id.* at 165.

23. The criminal law aspects are beyond the scope of this Comment, but for more information see Kerry Abrams & Brandon L. Garrett, *DNA and Distrust*, 91 Notre Dame L. Rev. 757 (2016) (discussing the effect of genetic information on constitutional rights). For more information about the Trump Administration's recent plans to collect DNA in federal detention facilities, see Caitlin Dickerson, *U.S. Government Plans to Collect DNA From Detained Immigrants*, N.Y. Times (Oct. 2, 2019), https://www.nytimes.com/2019/10/02/us/dna-testing-immigrants.html [https://perma.cc/5VT5-P9TV].

24. *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

25. *See* Drabiak, *supra* note 17, at 162.

26. *See infra* Section III.

27. *See infra* Section III.

28. Gauthier Chassang, *The Impact of the EU General Data Protection Regulation on Scientific Research*, ECancerMedicalScience (Mar. 1, 2017), https://ecancer.org/journal/11/full/709-the-impact-of-the-eu-general-data-protection-regulation-on-scientific-research.php [https://perma.cc/7Q94-EC38].

tential for privacy harms. Section III reviews some of the federal and state regulations that often apply to health data privacy. Section IV considers the strengths and weaknesses of the GDPR. Section V examines potential strategies for protecting genetic data and the benefits of the GDPR framework.

II.   Genetic Data

Effective privacy regulations require clear definitions. The following Section will provide a basic understanding of what genetic data is and how it is typically used to demonstrate why it is exceptionally sensitive and how the current regulations have gaps.

A.   *Defining Genetic Information and Data*

DNA is the inherited material contained in almost every cell in the human body, and it is made up of chemical building blocks.[29] Genes are the DNA sequences that give instructions for producing proteins.[30] A genome is the complete set of genetic instructions present in almost every cell.[31] The term "genetic information" is somewhat ambiguous and defined by various statutes in different ways.[32] Genetic data typically include the raw data obtained from sequencing, the report analyzing the raw data, and reported health data.[33] Genetic information can be anything that concerns individual genetic characteristics or family genetic characteristics.[34] Information obtained from DNA, self-reported health data, or analysis performed by a researcher—can all reveal information about genetics.[35]

Genetic testing is "any laboratory test of an individual's complete DNA, regions of DNA, chromosomes, genes, or gene products to de-

---

29. *What is DNA?*, Nat'l Insts. Health (Sept. 3, 2019), https://ghr.nlm.nih.gov/primer/basics/dna [https://perma.cc/SB62-9GJP].

30. Dennis Grishin et al., Blockchain-Enabled Genomic Data Sharing and Analysis Platform 5 (2018), http://arep.med.harvard.edu/pdf/Grishin_Church_v4.52_2018.pdf [https://perma.cc/H42L-KZBK].

31. *What is a Genome?* Nat'l Insts. Health (Sept. 3, 2019), https://ghr.nlm.nih.gov/primer/hgp/genome [https://perma.cc/7SDK-MX9H].

32. *See* Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, §101(d), 122 Stat. 881 (2008) (defining genetic information to include information about genetic test results for individuals and their families and manifestations of disease in their families). *But see* Nonprofit Healthcare Reform Act, Mich. Comp. Laws Ann. § 550.1401(9)(b) (West 2012) (defining genetic information as information about a gene, or gene product, or inherited characteristics from a gene test).

33. Future Privacy F., Privacy Best Practices for Consumer Genetic Testing Services 11 (2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf [https://perma.cc/Y4LA-3PFZ].

34. *Id*. at 13.

35. Susan Joung Rojahn, *Study Highlights the Risk of Handing Over Your Genome*, MIT Tech. Rev. (Jan. 17, 2013), https://www.technologyreview.com/s/509901/study-highlights-the-risk-of-handing-over-your-genome/ [https://perma.cc/9KHZ-UMWL].

termine the presence of the genetic characteristics in an individual or an individual's offspring."[36] Genetic testing involves collecting a sample of cells from a person—typically from hair, skin, blood, or saliva.[37] The sample is sent to a lab, where the DNA is separated from the other cells in the sample through DNA extraction.[38] Many of the popular direct-to-consumer genetic testing services involve a consumer purchasing a test tube with a barcode, submitting a saliva sample through the mail for processing in a lab, and then data from the lab are sent to the private company to interpret and communicate results with the consumer.[39]

There are several methods for analyzing genetic information in the lab. Genotyping is one method that finds variations in DNA sequences by comparing an individual sample to other samples.[40] Sequencing is another method that examines the order of the arrangement of DNA.[41] But there are many other interesting methods for analyzing individual differences in genes, including identifying the location of DNA within the nucleus[42] and studying the interactions between genes.[43]

In general, genetic sequencing involves identifying the order and arrangement of the building blocks of the chemical bases in an individual's DNA.[44] These arrangements are "instructions for making and maintaining a human being."[45] Variations in these arrangements

---

36. FUTURE PRIVACY F., *supra* note 33, at 11.

37. *Id.*

38. *What Happens to My Sample at the Laboratory?*, 23ANDME, https://customer-care.23andme.com/hc/en-us/articles/202904590-What-happens-to-my-sample-at-the-laboratory- (last visited Sept. 25, 2019) [https://perma.cc/JMW2-NRC2].

39. *Id.*

40. *Id.*

41. *What is DNA Sequencing?* NAT'L INSTS. HEALTH (Dec. 18, 2015), https://www.genome.gov/10001177/dna-sequencing-fact-sheet/ [https://perma.cc/UZ5A-CULK] [hereinafter *What Is DNA Sequencing?*].

42. *See* Elizabeth Pennisi, *Moving DNA to a Different Part of the Nucleus Can Change How it Works*, SCI. MAG. (Oct. 11, 2018, 11:00 AM), https://www.sciencemag.org/news/2018/10/moving-dna-different-part-nucleus-can-change-how-it-works [https://perma.cc/AF3Z-VNBK].

43. *See* John Quackenbush, *Using Networks to Link Genotype and Phenotype*, NAT'L INSTS. HEALTH (Mar. 5, 2018), https://prevention.nih.gov/education-training/methods-mind-gap/using-networks-link-genotype-phenotype [https://perma.cc/FUX4-EGXZ] ("Dr. Quackenbush's work has found that gene regulatory networks, and their structure, provide unique insight into how genetic elements interact with each other. He has also found that the structure of the network has predictive power for identifying single nucleotide polymorphisms (SNPs) likely to be associated with phenotype through genome-wide association studies.").

44. *What is DNA Sequencing?*, *supra* note 41 ("In the DNA double helix, the four chemical bases always bond with the same partner to form 'base pairs.' Adenine (A) always pairs with thymine (T); cytosine (C) always pairs with guanine (G). This pairing is the basis for the mechanism by which DNA molecules are copied when cells divide, and the pairing also underlies the methods by which most DNA sequencing experiments are done.").

45. *Id.*

(along with many other variables[46]) can convey information about an individual's physical features, their predisposition to certain conditions or diseases, and their current health.[47] All of this information can be stored electronically in databases and shared with others.[48]

B.   *Big Data and Genetics*

Information about individual genomes can be stored in various ways. Genomes can be coded in a database and made publicly available through a web portal.[49] Information about individual genomes in this format can easily be combined with other health data.[50]

Storing genetic information electronically results in a colossal amount of data. The human genome has 6.4 billion building blocks, including around 20,000 protein-coding genes.[51] One method that researchers use to make sense out of large amounts of data is data mining.[52] Data mining involves using algorithms and processes to analyze data and find patterns.[53] Data mining large genetic databases can help to efficiently identify variants, commonalities, and patterns in genetic information.[54] Through data mining, genetic data can also more easily be combined with other categories of data to better understand complex and rare traits.[55] Multiple sources help researchers achieve more statistically reliable data.[56] Since genetic traits are often the result of many factors, this research is especially suited for data-mining techniques.[57]

Research databases store and share genetic information in different ways. One example is the Genotype-Tissue Expression Project under

---

46. *See* Virginie Orgogozo et al., *The Differential View of Genotype–Phenotype Relationships*, Frontiers in Genetics (May 19, 2015), https://www.frontiersin.org/articles/10.3389/fgene.2015.00179/full [https://perma.cc/6SUU-PUSU] ("A difference in hair color could also be caused . . . by a combination of both genetic and non-genetic differences.").

47. *DNA Sequencing Fact Sheet*, Nat'l Insts. Health (Dec. 18, 2015), https://www.genome.gov/10001177/dna-sequencing-fact-sheet/ [https://perma.cc/GZ5K-PEUD] [hereinafter *DNA Sequencing Fact Sheet*].

48. *See* GeneWatch UK, The Data Protection Bill: Implications for DNA and Genetic Data 1 (Feb. 2018), http://www.genewatch.org/uploads/f03c6d66a9b354535738483c1c3d49e4/DPBill_GWbrief_Feb18.pdf [https://perma.cc/FL63-9TZQ].

49. Dankar et al., *supra* note 1, at 7.

50. *Id.*

51. Grishin et al., *supra* note 30, at 5.

52. *See* Marylyn D. Ritchie et al., *Methods of Integrating Data to Uncover Genotype–Phenotype Interactions*, 16 Nature Revs. Genetics 85, 88 (2015).

53. *See id.* at 88–89.

54. *See id.* at 85.

55. *Id.*

56. *Id.*

57. *Id.*

the National Institutes of Health.[58] Researchers around the world use this database to study the role of genetics in disease.[59] One researcher used this data to study how gene variants work together to determine observable traits.[60] He used the data to model and compare networks between groups of individuals and found "new drug targets, explored chemotherapy resistance, and investigated differences between the sexes."[61] Another example of a genetic research database is an online catalog with the specific mapped location of genetic variance, information about the observed disease and relevant research, and the clinical features of patients with that variance.[62] Anyone with an email address can get access to this information and can receive alerts about research updates to specific genes or diseases.[63] In early 2019, Children's Hospital of Philadelphia released an initial "8,000 DNA and RNA samples from children and families affected by pediatric cancers and structural birth defects" to the Kids First Data Resource Portal.[64] This new portal allows approved researchers to quickly access data relevant to rare pediatric diseases: imaging, genome sequencing, pathology slides, and surgery details.[65] The families give broad consent for sharing their information, and users are required to share their findings.[66]

C. *Genetic Data is Valuable*

Despite the potential for harm, genetic data sharing provides many benefits. Patients and consumers need to weigh the benefits and harms before undergoing genetic testing and sharing the results. The patient or consumer should decide that the benefits outweigh the potential harms before moving forward.

Many people have important and valid reasons for proceeding with genetic testing despite the potential harms. They might want to know about their own genetic information to understand their propensity for developing certain diseases, to learn about their probability of having a child with certain conditions, or to receive a more accurate diag-

---

58. *Genotype-Tissue Expression Project*, Nat'l Insts. Health, https://www.genome.gov/27543767/genotypetissue-expression-project-gtex/ (last visited Sept. 19, 2019) [https://perma.cc/2PV7-K4T5].

59. *See id.*

60. Quackenbush, *supra* note 43.

61. *Id.*

62. *See An Online Catalog of Human Genes and Genetic Disorders*, Online Mendelian Inheritance in Man, https://omim.org/ (last updated Aug. 28, 2019) [https://perma.cc/8M97-3VPP].

63. *See id.*

64. Neil Versel, *CHOP-Led 'Kids First' Portal Features Big Datasets Without Embargo*, Genomeweb (Jan. 14, 2019), https://www.genomeweb.com/informatics/chop-led-kids-first-portal-features-big-datasets-without-embargo#.XFXIXBlKhV8 [https://perma.cc/28CY-U5BB].

65. *Id.*

66. *Id.*

nosis from a doctor. People often move forward with testing because they want more information.

While individual genetic testing has numerous benefits, the benefits of sharing genetic data appear limitless. Large-scale genetic data sharing helps researchers identify variations in genetic makeup and the significance of those variations more efficiently.[67] Researchers can make connections between variations in genetic makeup. They can use those connections to explore the causes of different cancers, complex diseases, defects, and developmental delays.[68] One recent example involved a partnership between a research institute and a tech company to apply artificial intelligence to find patterns in different types of data.[69] Their first project will be combining genomic and sensor data to predict atrial fibrillation.[70] This is just one of many examples of how sharing genetic data can potentially save and improve lives.

This mass-sharing of data is especially important for detecting rare genetic variants that are more difficult to detect. The more people that provide their data, the more likely researchers can find a pattern in a variant. For example, a genetic variant for schizophrenia was not detected with 3,500 cases, was faintly identifiable with 10,000 cases, but was statistically significant with 35,000 cases.[71] More people sharing their genetic data increases the chances that researchers will find the causes behind rare diseases.

Besides the research benefits, individual physicians also benefit from large-scale sharing. Sharing genetic data helps to inform clinical care and can improve prevention, diagnosis, and treatment of disease.[72] Doctors can use data to identify risk factors for adverse reac-

---

67. *What are the Next Steps in Genomic Research?*, NAT'L INSTS. HEALTH (Oct. 1, 2019), https://ghr.nlm.nih.gov/primer/genomicresearch/nextsteps [https://perma.cc/7RQH-SW9V].

68. *DNA Sequencing Fact Sheet*, *supra* note 47.

69. Jessica Kim Cohen, *Scripps Partners with Nvidia to Apply AI to Genomic, Digital Sensor Data*, BECKER'S HEALTH IT & CIO REP. (Oct. 26, 2018), https://www.beckershospitalreview.com/artificial-intelligence/scripps-partners-with-nvidia-to-apply-ai-to-genomic-digital-sensor-data.html?origin=cioe&utm_source=cioe [https://perma.cc/PP7Q-H6RQ].

70. *Id. See also Atrial Fibrillation*, MAYO CLINIC (June 20, 2019), https://www.mayoclinic.org/diseases-conditions/atrial-fibrillation/symptoms-causes/syc-20350624 [https://perma.cc/89CF-T244] ("Atrial fibrillation is an irregular and often rapid heart rate that can increase your risk of strokes, heart failure and other heart-related complications.").

71. EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 7 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/42ZY-UHLA]; Manolis Kellis, *Big Data Opportunities & Challenges in Human Disease Genetics & Genomics*, BROAD INST. MIT & HARV. 13, http://web.mit.edu/bigdata-priv/ppt/ManolisKellis_Big_PrivacyBigData_CSAIL-WH.pptx (last visited Oct. 11, 2019) [https://perma.cc/5CGP-CL8R].

72. *See* Effy Vayena & Alessandro Blasimme, *Health Research with Big Data: Time for Systemic Oversight*, 46 J.L. MED. & ETHICS 119, 119 (2018).

tions to certain medications and prevent the adverse reaction.[73] Physicians can plan for the most effective treatment by using data to predict results.[74] Genetic data is extremely valuable, and its potential to improve healthcare is even more significant when shared on large scales.

D.   *Unique Privacy Concerns*

Although the benefits of sharing genetic data have proven remarkable, there are many privacy concerns with the current system. Genetic data is extremely sensitive because of how much it can reveal. Genetic data can "identify us, reveal our propensity to a range of diseases, and expose sensitive health information about biologically-linked family members."[75] Third parties that have access to this information potentially have "access to the innermost contents of your cells . . . ."[76] This includes access to an individual's ethnicity and heritage, physical features, predisposition to certain conditions or diseases, and current health status.[77] Additionally, genetic data is uniquely sensitive because the amount of information that can be conveyed increases with advances in technology and research.[78] Many researchers already claim they can predict a wide range of traits based on genetic information, including identification of sexual orientation, political behavior, criminality,[79] and intelligence.[80] The information obtainable from genetic data analysis continues to grow.

Second, there is a lack of transparency about the specific groups that will have access to the data and their purpose.[81] Because of rapidly developing technology and the enormous amount of potentially meaningful information available, many parties are interested in obtaining genetic data. Pharmaceutical companies, clinical researchers,

---

73. GRISHIN ET AL., *supra* note 30, at 7.

74. *What is Precision Medicine?*, NAT'L INSTS. HEALTH (Sept. 10, 2019), https://ghr.nlm.nih.gov/primer/precisionmedicine/definition [https://perma.cc/823G-9YSL].

75. Elizabeth R. Pike, *Securing Sequences: Ensuring Adequate Protections of Genetic Samples in the Age of Big Data*, 37 CARDOZO L. REV. 1977, 1980 (2016).

76. Charles Seife, *23andMe Is Terrifying, but Not for the Reasons the FDA Thinks*, SCI. AM. (Nov. 27, 2013), https://www.scientificamerican.com/article/23andme-is-terrifying-but-not-for-the-reasons-the-fda-thinks [https://perma.cc/2H4U-56AB].

77. Deborah Hellman, *What Makes Genetic Discrimination Exceptional*, 29 AM. J.L. & MED. 77, 88 (2003).

78. *See* Dankar et al., *supra* note 1, at 2.

79. Jennifer Lynch, *DNA Collection is Not the Answer to Reuniting Families Split Apart by Trump's "Zero Tolerance" Program*, ELECTRONIC FRONTIER FOUND. (July 10, 2018), https://www.eff.org/deeplinks/2018/07/dna-collection-not-answer-reuniting-families-split-apart-trumps-zero-tolerance [https://perma.cc/PFW8-N97X].

80. Antonio Regalado, *DNA Tests for IQ Are Coming, but It Might Not Be Smart to Take One*, MIT TECH. REV. (Apr. 2, 2018), https://www.technologyreview.com/s/610339/dna-tests-for-iq-are-coming-but-it-might-not-be-smart-to-take-one/ [https://perma.cc/63LC-UUQL].

81. *See* Drabiak, *supra* note 17, at 162–63.

employers,[82] insurance companies, hospitals, and law enforcement all might have varied interest in the information that genetic data can provide.[83] Consumers and patients may be interested in giving their genetic data to researchers to help discover cures for diseases, but may not be interested in helping a company make a profit by selling their genetic data.[84]

Third, patients and consumers may lose control of their genetic data in the current structure. Consent can help individuals learn about how their data might be used,[85] but many regulations seem to agree with the idea that "the right to privacy ceases . . . with . . . consent."[86] Requiring consent from individuals before sharing their data helps consumers to have more control, but researchers and companies often collect samples before they know exactly how the data will be used, whether the terms might change, and who might acquire the data later.[87] Consent may be too vague to give any amount of control if researchers and companies collect information without an exact plan for how it will be used and without specific information about who it will be shared with.[88] In addition, genetic information can implicate family members who never donated DNA and never consented to share any information.[89] Since genetic information can implicate family members who never consented, there is concern regarding whether an individual's consent for disclosure is enough.[90] Further, genetic variants are often reclassified.[91] The information that can be obtained from an individual's data only grows with time.[92] Since new discoveries can change the implications of genetic data, individuals may decide after sharing that they no longer want their data to be available. The

---

82. John P. Dever & James A. Dever, *A Democracy of Users*, 6 J.L. & Cyber Warfare 8, 18 (2017).

83. Drabiak, *supra* note 17, at 143.

84. Maggie Fox, *What You're Giving Away with Those Home DNA Tests: It's the Most Valuable Thing You Own*, NBC News (Nov. 29, 2017, 8:46 AM CST), https://www.nbcnews.com/health/health-news/what-you-re-giving-away-those-home-dna-tests-n824776 [https://perma.cc/UNR6-G6CV].

85. Wendy K. Mariner, *Mission Creep: Public Health Surveillance and Medical Privacy*, 87 B.U. L. Rev. 347, 372 (2007).

86. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 218 (1890).

87. *See* Vayena & Blasimme, *supra* note 72, at 121–22.

88. *Id.* at 120.

89. *See* Drabiak, *supra* note 17, at 162.

90. *Genetic Information Privacy*, Electronic Frontier Found., https://www.eff.org/issues/genetic-information-privacy (last visited Nov. 11, 2018) [https://perma.cc/52PQ-MR9P].

91. *See* Ciara Curtin, *At NSGC, Genetic Counselors Discuss Why, How Gene Variants Are Reclassified*, Genomeweb (Nov. 19, 2018), https://www.genomeweb.com/molecular-diagnostics/nsgc-genetic-counselors-discuss-why-how-gene-variants-are-reclassified#.XFcsyBlKhV8 [https://perma.cc/P2CP-RQZR].

92. *Id.*

lack of specific, informed consent ultimately results in people losing control of their genetic data.[93]

Fourth, genetic data available in databases provides a unique type of privacy and security risk because of the difficulty with anonymization.[94] Many regulations allow sharing anonymous data, but genetic data most likely cannot be anonymized.[95] For example, there are methods available to identify "anonymized" data.[96] The researchers behind one study found they could "deanonymize genomic data using only publicly available Internet information and some clever detective work."[97] Companies can buy "anonymized" health data and use new technology to deanonymize data.[98] Another study showed that even if you have never provided your own DNA to a database, you could be identified based on information provided by a distant relative.[99]

Finally, potential study participants often cite privacy concerns as a reason for not participating in research.[100] As a consequence, privacy concerns impede research. When people do not feel protected by the law and are concerned with how their data will be used, they are less likely to participate.[101] More protective data regulations may be justified sufficiently by guaranteeing security and privacy to encourage participation in research and to promote advancements in medicine.

III.   U.S. Regulations: Protections and Limitations

While different states disagree on exactly how much privacy protection individuals should be entitled to, every United States citizen has

---

93. *See* Fox, *supra* note 84.

94. *See* Dankar et al., *supra* note 1, at 7.

95. *Id.*

96. *Policy for Sharing of Data Obtained in NIH Supported or Conducted Genome-Wide Association Studies*, Nat'l Insts. Health (Aug. 28, 2007), https://nccih.nih.gov/node/9680 [https://perma.cc/3ZQR-NG2B].

97. Rojahn, *supra* note 35. *See also* Gina Kolata, *Web Hunt for DNA Sequences Leaves Privacy Compromised*, N.Y. Times (Jan. 17, 2013), https://www.nytimes.com/2013/01/18/health/search-of-dna-sequences-reveals-full-identities.html [https://perma.cc/U6ZL-UR49]; Melissa Gymrek et al., *Identifying Personal Genomes by Surname Inference*, 339 Sci. 321, 321 (2013).

98. John Hickey, *Advancement of Artificial Intelligence Opens Health Data Privacy to Attack*, Berkeley News (Dec. 21, 2018), https://news.berkeley.edu/2018/12/21/advancement-of-artificial-intelligence-opens-health-data-privacy-to-attack/ [https://perma.cc/NW2S-YXX2].

99. Jocelyn Kaiser, *We Will Find You: DNA Search Used to Nab Golden State Killer Can Home in on About 60% of White Americans*, Sci. Mag. (Oct. 11, 2018, 2:00 PM), https://www.sciencemag.org/news/2018/10/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white [https://perma.cc/VCY4-DRTX].

100. *See* Casie A. Genetti et al., *Parental Interest in Genomic Sequencing of Newborns: Enrollment Experience from the BabySeq Project*, Genetics Med. (Sept. 13, 2018), https://www.nature.com/articles/s41436-018-0105-6#article-info [https://perma.cc/7FF7-32SH].

101. *See* Adam Rogers, *The House Health Plan Makes Your Genes a Preexisting Condition*, Wired (May 4, 2017, 7:55 PM), https://www.wired.com/2017/05/house-health-plan-makes-genes-preexisting-condition/ [https://perma.cc/U5ME-7E7C].

certain protections provided by federal regulations. But complying with all regulations is challenging, and deciding which law applies in a particular situation is not always clear.

The following hypothetical demonstrates some complexities of the current privacy regulations: "Patient A" is an adult, living in the United States, who thinks he may be at risk for cancer and wants to get more information about his genetic predisposition to the disease. Patient A visits a local hospital for a blood test and subsequent genetic testing.[102] Patient A also sends his DNA to a direct-to-consumer genetic testing service. Additionally, Patient A wears a watch that tracks his heart rate and exercise.

Who regulates the collection, processing, and storage of Patient A's genetic data? What happens if Patient A shares data from the genetic company with his doctor? What if he shares data from his watch with his doctor, and it is stored with his genetic information in his medical record? Does the combination of new data change how it is regulated? Does Patient A retain any control over his data? Does he have a cause of action if there is a breach? If Patient A discovers that he has a propensity for a certain type of cancer, does the law protect him and prevent companies from using that information to make decisions?

A.   *Federal Regulations*

The United States has many regulations that offer some protection for patient and consumer privacy. However, the regulations are difficult to comply with because of their quantity and complexities, and there are still many gaps in privacy protection. Federal regulations are enacted to fix individual issues as they arise, with often very little consideration about future developments.[103] As a consequence, the various regulations are complex and disconnected.[104] The application of each regulation varies, dependent on the business structure or industry, the location of the parties, and how the data are used.[105]

---

102. There are many regulations that apply here that are beyond the scope of this Comment. For example, CLIA standards regulate the quality of the laboratory practices and FDA standards regulate the clinical validity of the tests. For more information about the various laws that apply in genomic research, see Leslie E. Wolf et al., *The Web of Legal Protections for Participants in Genomic Research*, 29 HEALTH MATRIX 1 (2019). For information about consumer data protection laws, see Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 2 (2018).

103. *See generally* Angela L. Morrison, *A Research Revolution: Genetic Testing Consumers Become Research (and Privacy) Guinea Pigs*, 9 J. TELECOMM. & HIGH TECH. L. 573 (2011).

104. *See generally id.*

105. *See id.* at 598–99.

1. HIPAA

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") is a federal law that regulates the use and disclosure of medical records and health information controlled by covered entities and their business associates.[106] The HIPAA Privacy Rule limits access to protected health information by restricting how that information can be released and requiring authorization.[107] Covered entities that are subject to HIPAA regulations include most providers of health plans and health care.[108] The statute provides a cause of action for the U.S. Department of Health and Human Services, Office for Civil Rights to enforce compliance through civil penalties and refers criminal violations to the Department of Justice.[109]

But HIPAA has many exceptions that result in gaps in privacy protection. For example, there are several exceptions that allow sharing information without authorization.[110] HIPAA permits disclosing genetic information without consent if the data have been de-identified.[111] The statute considers protected health information to be de-identified after removing eighteen identifying elements in the record, although many have argued that genetic data can never truly be anonymous.[112] In addition, HIPAA permits disclosing health information without authorization for "treatment, payment, and routine health care operations"; public health; "specialized government functions, including national security and intelligence operations"; law enforce-

---

106. *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996).

107. *HIPAA for Professionals*, U.S. Dep't Health & Hum. Servs. (June 16, 2017), https://www.hhs.gov/hipaa/for-professionals/ [https://perma.cc/5GC3-BVTU].

108. *Your Privacy Rights Under HIPAA*, Tex. L. Help, https://texaslawhelp.org/ article/your-privacy-rights-under-hipaa (last visited Oct. 11, 2018) [https://perma.cc/ 6FCG-6QKU].

109. *Enforcement Process*, U.S. Dep't Health & Hum. Servs. (June 7, 2017), https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/enforcement-process/index.html [https://perma.cc/VYE4-GXQU].

110. *See* Barbara J. Evans, *HIPAA's Individual Right of Access to Genomic Data: Reconciling Safety and Civil Rights*, 102 Am. J. Hum. Genetics 5, 7 (2018); Roberta B. Ness, *Influence of the HIPAA Privacy Rule on Health Research*, 298 J. Am. Med. Ass'n 2164, 2164 (2007); *HIPAA for Professionals*, *supra* note 107; 45 C.F.R. § 164.502(a)(1)(iv) (2015); *Does the HIPAA Privacy Rule Protect Genetic Information?*, U.S. Dep't Health & Hum. Servs. (Dec. 20, 2002), https://www.hhs.gov/ hipaa/for-professionals/faq/354/does-hipaa-protect-genetic-information/index.html html [https://perma.cc/GN4K-HDL2].

111. Morgan Leigh Tendam, *The HIPAA-POTA-MESS: How HIPAA's Weak Enforcement Standards Have Led States to Create Confusing Medical Privacy Remedies*, 79 Ohio St. L.J. 411 (2018); 45 C.F.R. § 164.502 (2015).

112. Jennifer Kulynych & Henry T. Greely, *Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights with Research When Privacy and Science Collide*, 4 J.L. & Biosciences 94, 115–16 (2017).

ment; and "judicial and administrative proceedings."[113] HIPAA also provides many research exceptions.[114] Finally, HIPAA is directed at covered entities, so genetic data processed and stored by non-covered entities typically have no HIPAA protection.[115]

2. GINA

The Genetic Information Nondiscrimination Act of 2008 ("GINA") is a federal regulatory program designed to protect against genetic discrimination by health insurers and employers.[116] GINA restricts health insurers and employers from using genetic information to make coverage or employment decisions.[117] The statute defines genetic information as "information about—(i) such individual's genetic tests, (ii) the genetic tests of family members of such individual, and (iii) the manifestation of a disease or disorder in family members of such individual."[118] The Equal Employment Opportunity Commission ("EEOC") investigates and enforces GINA claims.[119]

GINA may provide some protection against discrimination, but GINA does not apply to employers with less than fifteen employees,[120] military, or Indian Health Services.[121] It also does not apply to life insurance, disability insurance, or education.[122] GINA does not protect you if you already have symptoms or begin to show symptoms.[123] GINA does not prevent insurers from basing their decisions on current symptoms or a diagnosis of disease, even if a genetic test

---

113. *The Law and Medical Privacy*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/law-and-medical-privacy (last visited Nov. 11, 2018) [https://perma.cc/56VB-ZL2K].

114. *Id.*

115. *Id.*

116. Jessica L. Roberts, *Preempting Discrimination: Lessons from the Genetic Information Nondiscrimination Act*, 63 VAND. L. REV. 439, 440 (2010).

117. Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, § 202, 122 Stat. 881, 907 (2008).

118. *Id.* § 101, 122 Stat. at 885.

119. *What You Should Know: Questions and Answers About the Genetic Information Nondiscrimination Act (GINA) and Employment*, U.S. EQUAL EMP. OPPORTUNITY COMMISSION, https://www.eeoc.gov/eeoc/newsroom/wysk/gina_nondiscrimination_act.cfm (last visited Feb. 28, 2019) [https://perma.cc/9HS4-B7F3].

120. *Information Nondiscrimination Act of 2008*, U.S. EQUAL EMP. OPPORTUNITY COMMISSION, https://www.eeoc.gov/laws/regulations/gina_qanda_smallbus.cfm (last visited Sept. 20, 2019) [https://perma.cc/BXC8-6LEZ] [hereinafter *Information Nondiscrimination Act of 2008*].

121. *Genetic Information Nondiscrimination Act*, GENETIC ALLIANCE, THE GENETICS & PUB. POL'Y CTR. JOHNS HOPKINS U. & NAT'L COALITION FOR HEALTH PROF. EDUC. GENETICS (June 2010), http://www.ginahelp.org/GINAhelp.pdf [https://perma.cc/N6HW-H8ED] [hereinafter *Genetic Information Nondiscrimination Act*].

122. Sarah Zhang, *The Loopholes in the Law Prohibiting Genetic Discrimination*, ATLANTIC (March 13, 2017), https://www.theatlantic.com/health/archive/2017/03/genetic-discrimination-law-gina/519216/ [https://perma.cc/C3MJ-D8RZ].

123. *Information Nondiscrimination Act of 2008*, *supra* note 120; Rogers, *supra* note 101.

revealed the diagnosis.[124] For example, if genetic testing reveals that a person has a genetic mutation for a particular disease before showing symptoms of it, an insurer cannot use that information to make decisions about that person's coverage or premiums because of GINA.[125] But when they show symptoms of the disease, GINA no longer protects them.[126]

The Affordable Care Act ("ACA") fills this gap and prevents health insurers from discriminating based on preexisting conditions,[127] but the current political climate suggests that the ACA could be overturned.[128] If the ACA is overturned, GINA would prevent health insurance discrimination based on predicted diseases from genetic information, but nothing would prohibit health insurance discrimination after that person shows symptoms or is diagnosed with the predicted disease.[129]

3. The Federal Trade Commission

If an entity is not covered by HIPAA, it only has to protect privacy according to the much less stringent requirements of the Federal Trade Commission ("FTC"). The FTC protects consumers from unfair trade practices through regulation and enforcement of various laws.[130] Unfair practices are defined as those "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[131]

The FTC can bring actions against companies for being "deceptive" if the company does not follow its own privacy practices or protect consumer privacy adequately.[132] For example, the FTC alleged that Facebook committed unfair practices when the company shared information without informed consent—a practice contrary to prior statements that the company would give users more control over their information.[133] The FTC charged a different company for deceptive

---

124. *Genetic Information Nondiscrimination Act*, *supra* note 121.

125. *Id.*

126. *Id.*

127. Lorelei E. Walker & Mark A. Rothstein, *Are Genetic Discrimination Laws Up to the Task?*, MEDSCAPE (Aug. 8, 2012), https://www.medscape.com/viewarticle/7685 60#vp_2 [https://perma.cc/Q4WK-KVY3].

128. Vann R. Newkirk, *The Federal Government Abandons the Most Popular Part of the ACA*, ATLANTIC (June 8, 2018), https://www.theatlantic.com/politics/archive/2018/06/aca-preexisting-conditions-doj/562442/ [https://perma.cc/42YU-UQAA].

129. *See* Morrison, *supra* note 103.

130. *What We Do*, FED. TRADE COMMISSION, https://www.ftc.gov/about-ftc/what-we-do (last visited Jan. 11, 2018) [https://perma.cc/BWV2-EAFF].

131. 15 U.S.C. § 45(n) (2012).

132. SEDONA CONFERENCE, *Data Privacy Primer*, 19 SEDONA CONF. J. 273, 331 (2018).

133. Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 PENN ST. L. REV. 777, 789–90 (2016).

practices because it automatically collected information about the contacts on consumer phones, while a statement on the site implied that the company would only collect data about contacts if the user chose to do so.[134]

The FTC can also bring enforcement actions when a company's data security methods fail to protect sensitive consumer data, but there are significant limits on that right.[135] The Third Circuit Court of Appeals held that the FTC had the authority to enforce data security through its power to regulate unfair trade practices.[136] But the Eleventh Circuit Court of Appeals reversed an FTC finding that a laboratory's failure to maintain the security of customer data was an unfair practice because the FTC's order was vague.[137] The Eleventh Circuit held that an FTC order directing LabMD to create a more secure program was unenforceable because it did not direct LabMD to "stop committing a specific act," but rather required the company to "overhaul and replace its data-security program to meet an indeterminable standard of reasonableness."[138]

The FTC is especially limited if the company has set lax standards for its privacy policies. The FTC cannot likely take action against companies that directly tell consumers they will widely share user data.[139] "If users do not do their homework on what information their apps are collecting about them, and the app makers are not foolish enough to outright lie about what they are doing, the FTC's ability to control how companies share our data is very limited."[140]

B.   *State Regulations*

Many states have passed different laws to protect genetic privacy and prevent genetic discrimination. State laws vary widely in scope, applicability, and the protection provided. "Ten state constitutions reference a right to privacy: Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina, and Washington."[141] Several states define genetic information as the individual's personal property.[142] Some states prohibit genetic discrimination in life and dis-

---

134. Complaint for Civil Penalties, Permanent Injunction, and Other Relief at 4, *United States v. Path, Inc.*, No. C-13-0448 (N.D. Cal. filed Jan. 31, 2013).

135. SEDONA CONFERENCE, *supra* note 132, at 332.

136. Fed. Trade Comm'n v. Wyndham Worldwide Corp., 779 F.3d 236, 249 (3d Cir. 2015).

137. LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1237 (11th Cir. 2018).

138. *Id.* at 1223, 1236.

139. Lipman, *supra* note 133, at 790 ("For example, the company Groupon was relatively open about the fact that it was going to widely share its users' data (including their location) so the FTC could not take action against them for doing so.").

140. *Id.*

141. SEDONA CONFERENCE, *supra* note 132, at 331.

142. *See, e.g.*, Deborah L. McLochlin, *Whose Genetic Information Is It Anyway? A Legal Analysis of the Effects That Mapping the Human Genome Will Have on Privacy*

ability insurance.[143] Some restrict the redisclosure of genetic information to a third party without consent.[144] Some states have created consequences for an unlawful disclosure, including criminal and civil punishments and fines.[145]

California passed some of the strictest rules to protect data privacy and prevent discrimination. In 2018, California passed the California Consumer Privacy Act ("CCPA").[146] The statute applies to any "company that does any amount of business in California if the company collects or tells others to collect personal information of California residents . . . ."[147] The CCPA defines personal information broadly to include any "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[148] "This includes data from internet or network activity, such as browsing and search history; data from a consumer's interaction with a website, application, or advertisement; biometric and geolocation data; and any inferences that can be drawn from such information."[149] The statute gives consumers the right to request a business delete their personal information, the ability to opt out of businesses selling their information, and provides a private right of action for consumers.[150]

California also passed the California Genetic Information Nondiscrimination Act ("CalGINA") in 2011.[151] CalGINA prohibits genetic discrimination in several areas, including emergency medical services, mortgage lending, and education.[152] CalGINA also allows plaintiffs to recover monetary damages not subject to damages caps.[153]

Rights and Genetic Discrimination, 19 J. MARSHALL J. COMPUTER & INFO. L. 609, 634–35 (2001).

143. *See* Morrison, *supra* note 103, at 584.

144. Claire Marblestone, *Privacy Issues in the Sharing of Genetic Information*, FOLEY & LARDNER LLP (Sept. 18, 2014), https://www.foley.com/privacy-issues-in-the-sharing-of-genetic-information-09-18-2014/ [https://perma.cc/7MYZ-ZTPE].

145. *Id.*

146. *A Letter from Alastair Mactaggart, Board Chair, Californians for Consumer Privacy*, CALIFORNIANS FOR CONSUMER PRIVACY, https://www.caprivacy.org/about-us (last visited Feb. 28, 2019) [https://perma.cc/P7ZL-5DVN].

147. John Conley & Isaac Newell, *The Strictest Data Privacy Law in the U.S.*, PRIVACY REP. (July 31, 2018), https://theprivacyreport.com/2018/07/31/the-strictest-data-privacy-law-in-the-united-states/ [https://perma.cc/T32B-CG8Q].

148. California Consumer Privacy Act, CAL. CIV. CODE § 1798.140(o) (effective Jan. 1, 2020).

149. Conley & Newell, *supra* note 147.

150. *Id.*

151. California Genetic Information Nondiscrimination Act (CalGINA), S.B. 559, 2011 Leg. (Cal. 2011).

152. *Id.*

153. Nicole Baarts & Megha Charalambides, *A New Year, A New Wellness Program*, CAL. PECULIARITIES EMP. L. BLOG (Jan. 19, 2018), https://www.calpeculiarities.com/2018/01/19/a-new-year-a-new-wellness-program/ [https://perma.cc/9RVH-DTH8].

California has taken some big steps to protect the privacy of its citizens. But this creates compliance challenges for industries that process and store information for customers in multiple states.[154] The California regulations also create sharing and access problems because of the variance between states.[155]

IV.   GENERAL DATA PROTECTION REGULATION

The General Data Protection Regulation ("GDPR") is a comprehensive data regulation, promulgated by the European Union ("EU"), enforceable as of May 2018.[156] The regulation "standardizes data protection law across all twenty-eight EU countries and imposes strict new rules on controlling and processing personally identifiable information."[157] The GDPR was enacted to give individuals more rights, and the effects have been far-reaching.[158] The GDPR applies to any organization in any country that collects or processes the data of EU citizens; it has had a global influence.[159] American companies spent an estimated $7.8 billion preparing for the enforcement date of the GDPR.[160] Instead of complying with the GDPR, some companies closed.[161] Other companies have implemented GDPR protections internationally—protecting all of their customers, not just those in the EU.[162]

The regulation imposes stiff fines for non-compliance: up to $22 million or 4% of the worldwide annual revenue of the prior financial year.[163] The fine depends on ten criteria, among them: which articles

---

154. *Id.*

155. *Id.*

156. FUTURE PRIVACY F., *supra* note 33, at 11.

157. Kris Lahiri, *What is General Data Protection Regulation?*, FORBES (Feb. 14, 2018, 1:21 PM), https://www.forbes.com/sites/quora/2018/02/14/what-is-general-data-protection-regulation/#7e545ae562dd [https://perma.cc/7BDL-PVZ8].

158. *See* Kyle Petersen, *GDPR: What (and Why) You Need to Know About EU Data Protection Law*, 31 UTAH B.J. 12, 12 (2018).

159. *See generally id.*

160. Oliver Smith, *The GDPR Racket: Who's Making Money From This $9bn Business Shakedown*, FORBES (May 2, 2018 2:30 AM), https://www.forbes.com/sites/oliver-smith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shake down/#3b0ff15234a2 [https://perma.cc/VV2H-Q7MW].

161. Ivana Kottasová, *These Companies Are Getting Killed by GDPR*, CNN BUS. (May 11, 2018, 6:39 AM ET), https://money.cnn.com/2018/05/11/technology/gdpr-tech-companies-losers/index.html [https://perma.cc/T96A-SU5N].

162. *The EU General Data Protection Regulation*, HUM. RTS. WATCH, (June 6, 2018, 5:00 AM EDT), https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation [https://perma.cc/69EM-4XWK] ("Microsoft, Apple, and Twitter announced that they would extend . . . some of the regulation's protections to their customers worldwide.").

163. Kimberly A. Houser & W. Gregory Voss, *GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?*, 25 RICH. J.L. & TECH. 1, 60 (2018).

were violated, the nature of the data, whether it was intentional, and what preventative measures were taken.[164]

The GDPR requires that processors have a legal basis before processing personal data.[165] "Processing" is defined broadly and includes any action that involves coming into contact with data.[166] "Personal data" is defined as any information that can be used to identify someone.[167] A legal reason must be identified before ever coming into contact with any data that could identify someone.[168]

The GDPR puts significant limitations on data collection, processing, and storing. Data collection must be limited to only what is absolutely necessary, and processed with a specific purpose and high standard of transparency.[169] The GDPR requires companies to secure consumer data and to limit storage to a timeframe that is absolutely necessary.[170] The GDPR also provides individual citizens with the right to force companies to erase the personal data that the company has about them.[171]

The GDPR is framed as a regulation generally prohibiting anyone from processing sensitive data, with exceptions to that general rule.[172]

> Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.[173]

The regulation defines genetic data as:

---

164. *Fines and Penalties*, GDPR EU.ORG, https://www.gdpreu.org/compliance/fines-and-penalties/ (last visited Sept. 20, 2019) [https://perma.cc/WG2M-VS26].

165. JOHNS HOPKINS MED., PREPARING FOR THE EU GDPR IN RESEARCH SETTINGS 3 (2018), https://www.jhsph.edu/offices-and-services/institutional-review-board/_pdfs-and-docs/GDPR_Application%20in%20Research%20Settings.pdf [https://perma.cc/WL4Q-LUS9].

166. *Id.* at 8.

167. Matt Burgess, *What Is GDPR? The Summary Guide to GDPR Gompliance in the UK*, WIRED (Jan. 21, 2019), http://www.wired.co.uk/article/what-is-*gdpr*-uk-eu-legislation-compliance-summary-fines-2018 https://perma.cc/CJ9D-LG39].

168. *Monthly Newsletter GDPR: Accountability Privacy by Design and Privacy by Default*, DENTONS BOEKEL (Apr. 18, 2017), https://dentons.boekel.com/en/insights/alerts/2017/april/18/monthly-newsletter-gdpr-accountability-privacy-by-design-and-privacy-by-default [https://perma.cc/8CZ2-KKSG].

169. *Id.*

170. *Id.*

171. Burgess, *supra* note 167.

172. Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What It Is and What It Means*, 28 INFO. & COMM. TECH. L. 65, 82 (2019).

173. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L119) 1, art. 9 [hereinafter GDPR].

> [I]nherited or acquired genetic characteristics of a natural person
> which give unique information about the physiology or health of
> that natural person and which result, in particular, from an analysis
> of a biological sample from the natural person in question . . . or
> from the analysis of another element enabling equivalent informa-
> tion to be obtained.[174]

Processing data in one of these special categories is prohibited, un-
less one of ten exemptions apply.[175] But even if an exemption applies,
there must still be a legal basis for processing.[176] Exemptions allow
processing sensitive data when it is necessary for public health, scien-
tific research, or when explicit consent is given.[177] One exception is
when explicit consent is obtained from the subject, defined as a
"freely given, specific, informed, and unambiguous indication of the
data subject's wishes by which he or she, by a statement or by a clear
affirmative action, signifies agreement to the processing of personal
data relating to him or her."[178] Consent requires an action; clicking a
box or choosing a setting might be enough, but "pre-ticked boxes (in-
activity) [does] not constitute consent."[179] Even if there is explicit con-
sent, subjects may withdraw consent at any time.[180]

The GDPR also distinguishes between types of data that can be
anonymized. GDPR does not regulate anonymous data—data that
can no longer be identified.[181] The GDPR defines whether data are
identifiable broadly, considering available technology.[182] Whether
data are identifiable under the rule requires looking at "all the means
of identification . . . reasonably likely to be used by any person."[183]
Whether a method is "reasonably likely to be used" involves an analy-
sis of the cost and time required and the available technology.[184] Ap-
plying this definition currently, there could be anonymous genetic
data not subject to regulation that could be shared openly.[185] For ex-

---

174. Chassang, *supra* note 28, at 5.

175. GDPR, *supra* note 173.

176. Itsiq Benizri, Martin Braun & Frédéric Louis, *The Legal Basis for Processing Personal Data in the Context of Clinical Trials in the EU: The European Data Protection Board Provides Some Clarifications, but Questions Remain*, JD Supra (Feb. 20, 2019), https://www.jdsupra.com/legalnews/the-legal-basis-for-processing-personal-39916/ [https://perma.cc/QX6X-Z4M2].

177. GDPR, *supra* note 173.

178. *Id.* art. 4(11).

179. *Monthly Newsletter: GDPR The Concept of Consent*, Dentons Boekel (Feb. 23, 2017), https://dentons.boekel.com/en/insights/alerts/2017/february/23/monthly-newsletter-gdpr-the-concept-of-consent [https://perma.cc/4NXY-HUPE].

180. GDPR, *supra* note 173, art. 7(3).

181. *See* Mark Phillips, *Can Genomic Data Be Anonymized?*, Global Alliance Genomics & Health (Oct. 10, 2018), https://www.ga4gh.org/news/can-genomic-data-be-anonymised/ [https://perma.cc/A2E3-DQBB].

182. *Id.*

183. *Id.*

184. Phillips, *supra* note 181.

185. *Id.*

ample, it is possible that genetic variants specific to certain cancer cells could be anonymous in some instances.[186] By comparison, coded genomic sequence datasets remain protected personal data under the GDPR.[187] These coded data sets would likely be defined as pseudonymized data that can "no longer be attributed to a specific data subject without the use of additional information."[188] The GDPR regulates data given codes or pseudonyms as identifiable personal data.[189]

The GDPR increases the privacy rights and protections for EU citizens. The regulation limits unnecessary processing and provides a private right of action for individuals whose rights have been violated.[190] To pursue a cause of action, individuals only have to prove their information was not processed within the limits of the law and no further harms.[191]

But the GDPR has many critics with valid arguments. For example, the terms of the GDPR are expensive to comply with.[192] The significant costs associated with compliance could lead to a disadvantage for smaller companies with less resources.[193] There are also ambiguities in the regulation: the GDPR requires "reasonable" protection of personal data without clearly defining what constitutes reasonable.[194] This could create problems with both compliance and enforcement.[195] Further, some have suggested that the research exemption for processing sensitive data may be too broad.[196] Defining the research exception may be left up to the EU states and cause more confusion with regard to compliance.[197]

V.   ADOPTING A FEDERAL DATA PRIVACY REGULATION

Sharing genetic data can be useful in the right hands, but it involves many privacy concerns and risks. Individuals can use this information to improve medical treatment, and researchers can learn more about

---

186. *Id.*
187. *Id.*
188. JOHNS HOPKINS MED., *supra* note 165, at 2.
189. Phillips, *supra* note 181.
190. Burgess, *supra* note 167.
191. GDPR, *supra* note 173, art. 82(1).
192. *See* Kottasová, *supra* note 161.
193. *Id.*
194. Mike Meikle, *GDPR's First 150 Days Impact on the U.S.*, THREATPOST (Nov. 1, 2018, 5:31 PM), https://threatpost.com/gdprs-first-150-days-impact-on-the-u-s/138739/ [https://perma.cc/VWT8-BV8B].
195. *Id.*
196. Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1012–15 (2017).
197. Rita T. Lawlor, Zisis Kozlakidis, & Marianna Beldsoe, *GDPR in Biobanking for Precision Medicine Research: The Challenges*, OPEN ACCESS GOV'T (Nov. 14, 2018), https://www.openaccessgovernment.org/gdpr-in-biobanking-for-precision-medicine/54468/ [https://perma.cc/U63V-T57M].

rare diseases, but these important uses do not completely negate the duty to protect individual privacy.

Although there is some ambiguity about where a person's privacy entitlements truly come from, courts have held that medical and health information are entitled to privacy.[198] "An individual has a constitutional right to privacy which protects 'the individual interest in avoiding disclosure of personal matters.'"[199] In *United States v. Westinghouse Electric Corporation*, the Third Circuit Court of Appeals held that "an employee's medical records, which may contain intimate facts of a personal nature, are well within the ambit of materials entitled to privacy protection."[200] In *Whalen v. Roe*, the Supreme Court held that "the doctor-patient relationship is one of the zones of privacy accorded constitutional protection."[201] However, the concurring opinion by Justice Stewart stated there is no "general constitutional right to privacy," but the general right "to be left alone by other people" is determined by the individual states.[202] These cases share the idea that medical information should be private, even if there is not agreement about where the right should ultimately come from. But these cases were decided before private companies—often outside of the doctor-patient relationship—began obtaining, processing, storing, and sharing genomic data on very large scales.[203]

Because genetic data present unique privacy risks, finding a solution is challenging. There have been many solutions proposed.[204] One solution proposed extending HIPAA data portability requirements to any

---

198. *See* United States v. Westinghouse Elec. Corp., 638 F.2d 570, 577 (3d Cir. 1980).

199. Doe v. Delie, 257 F.3d 309, 315 (3d Cir. 2001) (quoting Whalen v. Roe, 429 U.S. 589, 599 (1977)).

200. *Westinghouse Elec. Corp.*, 638 F.2d at 577.

201. Whalen v. Roe, 429 U.S. 589, 596 (1977).

202. *Id.* at 607–08 (Stewart J., concurring) (quoting Katz v. United States, 389 U.S. 347 (1967)).

203. *See* Drabiak, *supra* note 17, at 160 ("The massive paradigm shift from collecting genomic and health information in the healthcare setting to the commercial arena means the transaction . . . may occur outside the scope of regulatory structures designed to protect health data privacy and to ensure that companies have consumers' informed consent when they provide DNA.").

204. *See generally* Natalie Ram, *DNA by the Entirety*, 115 Colum. L. Rev. 873 (2015) (discussing property rights in DNA); Sejin Ahn, *Whose Genome is it Anyway? Re-Identification and Privacy Protection in Public and Participatory Genomics*, 52 San Diego L. Rev. 751, 804–05 (2015) (treating DNA as personal property and limiting with a digital signature); Jane Yakowitz Bambauer, *The New Intrusion*, 88 Notre Dame L. Rev. 205 (2012) (allowing tort recovery under the tort of intrusion); Bartha Maria Knoppers, *Framework for Responsible Sharing of Genomic and Health-Related Data*, 8 Hugo J. 1, 6 (2014) (various frameworks and best practices); Amy L. McGuire et al., *Confidentiality, Privacy, and Security of Genetic and Genomic Test Information in Electronic Health Records: Points to Consider*, 10 Genetics Med. 495, 496–97 (2008) (discussing considering certain characteristics when developing policies such as predictive capability, immutability, and uniqueness).

entity that manages health data[205] with "[t]he goal [of] uniformity of data access policy, regardless of covered entity, business associate, or other commercial status."[206] The numerous, diverse proposals illustrate the complexity in finding an adequate solution.

The ideal solution would give individuals control and privacy while promoting research and innovation. Adopting a federal data privacy regulation for sensitive data could protect individuals better than our current regulations.[207] A general prohibition on processing sensitive data would be more protective of individual privacy.[208] The United States could adopt a regulation broad enough to adapt to changes in technology, but narrow enough to protect privacy and allow for medical innovation.

A. *Upstream Privacy Protection*

The various regulations that protect the privacy of American citizens are not really privacy regulations, but function as data use and disclosure rules.[209] Regulations in the United States seem to be more concerned with the industry that the company is in and less concerned with the nature of the data and how it is being used.[210] For example, the current federal regulations are more protective of health data when a doctor's office or hospital is processing genetic data and less protective when a company has the data.[211] This is probably not because individuals trust private companies more than their doctors but rather is a result of sector-specific regulations.

One way of viewing data protection models is *downstream* and *upstream*.[212] Upstream data protection models regulate collection.[213] In an upstream model, privacy is a concern at the earliest stages of collection, before the data are obtained.[214] Downstream models regulate disclosure after data are obtained or stored.[215] Downstream models

---

205. Jessica Kim Cohen, *HIPAA Changes Needed, According to Health IT Trade Groups*, Becker's Health IT & CIO Rep. (Dec. 6, 2018), https://www.beckershospitalreview.com/cybersecurity/hipaa-changes-needed-according-to-health-it-trade-groups.html?origin=cioe&utm_source=cioe [https://perma.cc/7UQA-JS67].

206. *HIPPA Modernization Needed, Experts Say*, AMIA (Dec. 5, 2018), https://www.amia.org/news-and-publications/press-release/hipaa-modernization-needed-experts-say [https://perma.cc/UN3S-M5F5].

207. *See* Johns Hopkins Med., *supra* note 165, at 1.

208. *Id.*

209. *See* Johns Hopkins Med., *supra* note 165, at 2.

210. *See* Johns Hopkins Med., *supra* note 165, at 6.

211. *See id.* at 9.

212. Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 Health Matrix 65, 66 (2014).

213. *Id.*

214. *Id.*

215. *Id.*

often protect collected data by restricting disclosure and requiring certain security standards.[216]

The majority of United States healthcare privacy regulations are downstream models that regulate use and disclosure.[217] Federal privacy rules regulate according to the sector the company is in.[218] HIPAA regulates downstream because it controls how information can be disclosed.[219] HIPAA "imposes physical and technological constraints on patient data storage designed to make it difficult for those outside of the health care system to acquire such data without consent."[220]

By comparison, the GDPR is an upstream model.[221] It is an overall ban on processing sensitive data, with exceptions to the overall rule.[222] Under the GDPR, certain measures have to be implemented before data can be collected.[223] The controller must decide the lawful basis for collecting data prior to collection.[224] Thus, data privacy is a concern in the beginning stages of designing products and before collection.[225]

Restricting who can process genetic data may protect individual privacy better and make discrimination less likely.[226] Rather than relying on what sector the company is in or what harms have occurred, in an upstream model, there is a limit on obtaining the data in the first place.[227] Moreover, while genetic data is a type of "health data," there are many parties interested in obtaining genetic data that are not in the healthcare sector.[228] Proving that a party obtained genetic data and used it to discriminate is very difficult.[229] Limiting who can process sensitive data may make discrimination less likely by not only limiting access, but also by not requiring an individual to prove discrimination to have a cause of action.[230] An entity processing genetic data (when an exception does not apply) breaks the law, and no further harms have to be proven.[231]

---

216. *Id.* at 103.

217. *Id.* at 67.

218. *Id.* at 89.

219. *Id.* at 68.

220. *Id.*

221. *See id.* at 105.

222. Hoofnagle et al., *supra* note 172.

223. *See* Petersen, *supra* note 158, at 16.

224. *See id.*; *see also* Benizri, Braun & Louis, *supra* note 176.

225. *See* Petersen, *supra* note 158, at 15.

226. *See generally* Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, 91 Wash. L. Rev. 703 (2016).

227. *See* Petersen, *supra* note 158, at 16.

228. *See* Vayena & Blasimme, *supra* note 72, at 121; Drabiak, *supra* note 17, at 145.

229. *See* Sonia M. Suter, *The Allure and Peril of Genetic Exceptionalism: Do We Need Special Genetics Legislation?*, 79 Wash. U. L.Q. 669, 717–18 (2001).

230. *See id.*

231. GDPR, *supra* note 173, art. 82(1) (providing a private right of action to enforce data privacy rights).

B. *Adaptability*

A federal regulation for sensitive data would protect individual privacy best if it is adaptable. First, it will likely remain effective if it is broad and based on core principles that promote privacy.[232] Regulations based on principles are more likely to remain effective in sectors that are developing and changing quickly.[233] Over time, narrow rules may be less effective; the results become more likely to deviate from legislative intent.[234] Narrow rules are also more likely to be unfairly applied among industries.[235]

Compared to adopting another narrow rule in one limited sector, a regulation framed similarly to the GDPR would be more effective over time.[236] The GDPR rules are broad, and they are based on core principles of individual rights and privacy protection.[237] The GDPR lists 173 Recitals[238] that establish principles ranging from "data protection is a fundamental right" to "the protection of personal data . . . balanced against other fundamental rights."[239] The GDPR prohibition on processing sensitive data is broad and based on a core principle: that sensitive data "merit specific protection" because of the inherent risks to "fundamental rights and freedoms."[240]

The GDPR rules also have broad, inclusive definitions.[241] The GDPR broadly defines "processing" as any operation or action that involves coming into contact with data.[242] By comparison, HIPAA defines "use" specifically, including sharing, applying, and examining.[243] HIPAA's narrow definition creates loopholes; it provides more opportunities for entities to process data without violating the statute.[244]

Second, a regulation allowing patients to revoke their data could adapt to the constant advances that increase the amount of information obtainable from genetic data.[245] Knowledge about genetic predispositions to traits and diseases grows with technology and research.[246] This undetermined future progression makes it impossible "to quantify the amount and sensitivity of personal information that can be

---

232. *Id.* recitals 1, 4.
233. *Regulation & the Economy: The Relationship & How to Improve It*, Committee for Econ. Dev. (Sept. 27, 2017), https://www.ced.org/reports/regulation-and-the-economy [https://perma.cc/NK6D-5S7Z].
234. *Id.*
235. *Id.*
236. *See id.*
237. GDPR, *supra* note 173, recitals 1, 2.
238. *Id.* recitals 1–173.
239. *See id.*
240. *Id.* recital 51.
241. *See id.* art. 4.
242. *Id.*
243. 45 C.F.R. § 160.103 (2018).
244. *See id.*
245. McGuire et al., *supra* note 204, at 495, 499.
246. *Id.* at 497.

derived from [genomic data]."[247] Patients and consumers should be able to share this information if they choose to, but should be able to revoke their consent if the changes make it something they no longer want to share.

Third, a regulation with broad definitions could adapt to the expanding uses of genetic data.[248] Genetic analysis continues to integrate with other health records.[249] Further, many types of health data can implicate genetics.[250] The line between health data and genetic data is difficult to separate; recent advancements have further blurred this line.[251] In 2012, the FTC "acknowledged . . . that 'the traditional distinction between [personally identifiable information and non-personally identifiable information] has blurred' and suggested that 'it is appropriate to more comprehensively examine data to determine the data's privacy implications.'"[252] The FTC looked at consumer data that could "be reasonably linked to a specific . . . device" instead of regulating particular categories.[253] Similarly, a regulation with broad definitions could protect individual privacy in a time of massive collection and storage of various data that can be connected and used in novel ways.[254]

Finally, a new regulation could protect privacy by solving some of HIPAA's problems with identifiable data. Similar to the GDPR, the regulation could be flexible and accommodate changes by considering available technology when defining anonymous data.[255] HIPAA specifies how to deidentify information while the GDPR definition does not.[256] HIPAA allows researchers to remove certain information from datasets and share the data, despite evidence that it can likely be reidentified.[257] "A data set that is 'de-identified' under HIPAA is not necessarily anonymized under the GDPR."[258] The GDPR analysis for determining whether data is identifiable is adaptable.[259] When data

---

247. Dankar et al., *supra* note 1, at 2.

248. McGuire et al., *supra* note 204, at 498.

249. *Id.* at 495.

250. *Id.* at 496.

251. *See id.* at 496, 498.

252. Alexander E. Reicher & Yan Fang, *FTC Privacy and Data Security Enforcement and Guidance Under Section 5*, J. Antitrust UCL & Privacy Sec. St. B. Cal. (2016), https://www.law.berkeley.edu/php-programs/jsp/fileDL.php?fID=5347 [https://perma.cc/2ARY-JEWZ] (quoting Fed. Trade Comm'n, Protecting Consumer Privacy In An Era Of Rapid Change: Recommendations For Businesses And Policymakers 19 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [https://perma.cc/5KHC-DGC2]).

253. *Id.*

254. Dankar et al., *supra* note 1, at 2.

255. GDPR, *supra* note 173, recital 26.

256. Johns Hopkins Med., *supra* note 165, at 2.

257. *Id.*

258. *Id.*

259. *Id.*

become identifiable because of a change in technology, it is no longer anonymous under the GDPR rules.[260]

VI.   Conclusion

The GDPR was adopted to replace the numerous, conflicting data protection laws of various EU states.[261] The GDPR gives individuals more control and more privacy at a critical time: when companies are pervasively capturing, sharing, and selling private genetic information and with rapid technology development.[262] The "GDPR is fundamentally different from U.S. regulations" because it requires companies to "respect & empower [its] customers."[263] Many U.S. citizens and companies have called for a regulation similar to the GDPR.[264]

Individual privacy protections are especially important with pervasive collection and storing, but individual privacy has to be balanced with the desire to promote innovation and improve healthcare. A new data regulation could provide privacy protection despite rapid developments. The regulation could be narrow enough to promote innovation, but broad enough to continue to protect privacy despite changes in technology. The regulation could give people more control and provide protection from discrimination.[265] People are hesitant to participate in research when they are not sure what will happen to their data and when they are not confident that the current regulations will protect them.[266] A new regulation could give people more confidence that their rights are protected and that they will retain some control over future uses of their data. A more protective regulation could give people more incentive to participate in research projects.

DNA tests provide genetic information that can cause social stigma[267] and provide information about a person's most private medical information.[268] But the current state of data collection research implicates other health data along with genetics.[269] A new regulation

---

260. GDPR, *supra* note 173, recital 26.

261. *See* Petersen, *supra* note 158, at 12.

262. *Id*. at 15.

263. Mike Lloyd, *The Biggest GDPR Mistake U.S. Companies Are Making*, Forbes (June 12, 2018, 7:30 AM), https://www.forbes.com/sites/forbestechcouncil/2018/06/12/the-biggest-gdpr-mistake-u-s-companies-are-making/#33cb404969f0 [https://perma.cc/Q5LE-ZDXU].

264. James Vincent, *Tim Cook Warns of 'Data-Industrial Complex' in Call for Comprehensive US Privacy Laws*, Verge (Oct. 24, 2018, 5:08 AM EDT), https://www.theverge.com/2018/10/24/18017842/tim-cook-data-privacy-laws-us-speech-brussels [https://perma.cc/G43G-TXCM].

265. Jessica L. Roberts, *The Genetic Information Nondiscrimination Act as an Antidiscrimination Law*, 86 Notre Dame L. Rev. 597, 645–47 (2013).

266. *See* Genetti et al., *supra* note 100.

267. James P. Evans & Wylie Burke, *Genetic Exceptionalism. Too Much of a Good Thing?* 10 Nature 500, 500 (2008).

268. *See* Drabiak, *supra* note 17, at 143.

269. *See id.* at 147.

should not just consider the known, current uses of genetic data. The regulation should be broad enough to consider future unknown uses.

A new regulation could increase the rights of individuals in relation to their data, limit unnecessary processing, and provide more clarity for compliance.[270] Under the proposed legislation, whether a patient visits a local hospital for a blood test and subsequent genetic testing or sends his DNA to a popular direct-to-consumer genetic testing service, the person retains ultimate control over their data. If they travel to a different state or transfer the data to another company, their data continue to be protected.

A new regulation could replace the incoherencies and disjointedness of the federal, state, and sector-specific regulations with a regulation that applies to everyone and adapts over time. Not only would it give more uniformity and clarity to individuals, businesses, and government entities, it would likely be applicable and adaptable to future developments and undetermined future scenarios. The current regulations have not adapted to innovation. The United States needs to enact legislation that considers the current state of genetic data processing and health privacy protection. The United States could protect and empower its citizens by learning from the EU model and adopting a federal privacy regulation.

---

270. Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the 23rd Computers, Freedom, and Privacy Conference: Reclaim Your Name (June 26, 2013), http://www.ftc.gov/speeches/brill/130626computersfreedom.pdf   [https://perma.cc/8FXL-6CWN].