THE DATA WE LEAVE BEHIND: LIMITS OF LEGAL PROTECTIONS FOR NEUROTECHNOLOGY AND GENOMIC DATA

Robert I. Field∗

ABSTRACT

It is almost impossible to go through a day without leaving digital traces through activities ranging from web searches to social media postings to use of smart phone apps. These traces permit providers of web-based services to amass large amounts of personal information that can be used to discern a user's interests, attitudes, preferences, behaviors, and other characteristics. In recent years, the companies that provide these services have begun to collect new kinds of especially sensitive biometric information, first reflecting genetic makeup and more recently reflecting neurotechnology measures of brain activity. Data on individual genetic traits and on entire genomes reveal the underlying nature of our physiological makeup, and brain data can reveal our innermost thoughts, even unconscious ones. Both kinds of data are collected on a wide scale by companies that offer testing services to customers on a direct-to-consumer (DTC) basis.

While these data are enabling tremendous medical advances, they also create new risks should they be improperly disclosed, including discrimination, psychological, and social stress from unwanted revelations, and identification of third parties. Privacy has been recognized as a human right for almost a century, both in global covenants and in American laws. However, the laws that protect privacy in the United States leave significant gaps, especially regarding personal data collected by DTC testing companies. At the same time, personal data have tremendous economic value, creating

∗ Professor of Law, Thomas R. Kline School of Law and Professor of Health Management and Policy, Dornsife School of Public Health, Drexel University. PhD Boston University, MPH Harvard Chan School of Public Health, JD Columbia Law School, AB Harvard College *magna cum laude*. The author extends grateful thanks to Hannah Segota for invaluable research assistance.

an incentive for companies to collect as much as possible. Proposed federal legislation would tighten legal oversight, but, even if enacted, its protections are limited regarding data sharing with external entities and risks to third parties. This Article proposes further reforms that would mandate standardized privacy policies for DTC testing companies that clearly disclose data protection procedures and limit data sharing with outside parties. Nevertheless, these and other new legal safeguards must be designed carefully so they protect individuals without jeopardizing opportunities for continued medical advances.

TABLE OF CONTENTS

INTRODUCTION

It is almost impossible to go through a day in any developed country without scattering a trail of personal information.[1] Almost any interaction with the internet leaves a record of the websites visited, the information searched for, the links clicked, and the personal reflections posted.[2] That information is available both to the websites visited through cookies left on hard drives and to the internet service providers (ISPs) that connect users to the World Wide Web.[3] But even if people stay offline, their daily activities are being monitored.[4] Credit card companies maintain records of purchases, including what was bought, from whom and where.[5] Cable television providers track the shows viewers watch and for how long.[6] Public cameras observe people using facial recognition.[7]

Nevertheless, most people disclose much more than necessary. Websites and apps that offer a broad range of services ask users to voluntarily submit personal information that is then retained and analyzed.[8] Among the countless variety of services, some arrange dates, some calculate mortgage payments, some estimate the value of homes, and

1. *See* Nica Latto, *A Day in Your Digital Life… and the Trail You Leave*, AVG: SIGNAL BLOG, https://www.avg.com/en/signal/digital-day-in-the-life (Aug. 17, 2022).

2. *See id.* Some websites loaded on mobile browsers collect information from device sensors without the user's knowledge or permission. Lily Hay Newman, *Mobile Websites Can Tap into Your Phone's Sensors Without Asking*, WIRED (Sept. 26, 2018, 9:00 AM), https://www.wired.com/story/mobile-websites-can-tap-into-your-phones-sensors-without-asking/.

3. *See Your ISP Is Tracking Every Website You Visit: Here's What We Know*, PRIV. POL'YS, https://www.privacypolicies.com/blog/isp-tracking-you/ (July 1, 2022).

4. *See* Burt Helm, *Credit Card Companies Are Tracking Shoppers Like Never Before: Inside the Next Phase of Surveillance Capitalism*, FASTCOMPANY (May 12, 2022), https://www.fastcompany.com/90490923/credit-card-companies-are-tracking-shoppers-like-never-before-inside-the-next-phase-of-surveillance-capitalism.

5. *Id.*

6. SLA, *How Cable Companies Are Using Data to Compete with Digital*, HARV. BUS. SCH. DIGIT. INNOVATION & TRANSFORMATION, https://d3.harvard.edu/platform-digit/submission/how-cable-companies-are-using-data-to-compete-with-digital/ (Apr. 9, 2018).

7. *Facial Recognition: Who's Tracking You in Public?*, CONSUMER REPS., https://www.consumerreports.org/privacy/facial-recognition-who-is-tracking-you-in-public1-a7157224354/ ((Dec. 30, 2015).

8. Latto, *supra* note 1.

some track user locations.[9] Use of such services involves no monetary charge, but customers pay by revealing personal data that can then be sold to marketers and others who use it to send targeted advertisements and other messages.[10] Personal harm from such disclosures is possible, although in most cases it is likely to be limited.[11]

However, a range of newer services collect personal information whose disclosure presents a qualitatively different and more serious risk of harm. These are services that collect health data, much of which includes biometric information that can identify the user.[12] Some services measure indicators of health status, for example blood pressure, pulse rate, and exercise activity through smart watches and smart phone apps.[13] Others collect highly personal information about our physiological and psychological traits.[14] In 2006, a commercial testing company known as 23andMe began offering analysis of the entire genome of customers for a fee.[15] Genomes contain the entire set of deoxyribonucleic acid (DNA) that determines the

9. *See, e.g.*, *Mortgage Calculator*, MORTG. CALCULATOR, https://www.mortgagecalculator.org (last visited Apr. 12, 2023); *Online Calendar Planner*, DAYVIEWER, https://dayviewer.com (last visited Apr. 12, 2023); *User Guide: Location Tracking*, BRAZE, https://www.braze.com/docs/user_guide/engagement_tools/locations_and_geofences/location_tracking/ (last visited Apr. 12, 2023).

10. *See Microtargeting*, INFO. COMM'R OFF., https://ico.org.uk/your-data-matters/be-data-aware/social-media-privacy-settings/microtargeting/ (last visited Apr. 12, 2023); *Your Data Is Shared and Sold … What's Being Done About It?*, KNOWLEDGE AT WHARTON (Oct. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/.

11. *But see* Silvia Milano, *Targeted Ads Aren't Just Annoying, They Can Be Harmful. Here's How to Fight Back*, FAST COMPANY (July 31, 2021), https://www.fastcompany.com/90656170/targeted-ads-arent-just-annoying-they-can-be-harmful-heres-how-to-fight-back.

12. *See* Gioacchino Tangari, Muhammad Ikram, Kiran Ijaz, Mohamed Ali Kaafar & Shlomo Berkovsky, *Mobile Health and Privacy: Cross Sectional Study*, 373 BMJ 439, at 1 (2021).

13. Francisco de Arriva-Perez, Manuel Caeiro-Rodriguez & Juan M. Santos-Gago, *Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-Use Scenarios*, BASEL (SENSORS), Sept. 2016, at 1, 1.

14. *See* Darius Štitilis & Marius Laurinaitis, *Treatment of Biometrically Processed Personal Data: Problem of Uniform Practice Under EU Personal Data Protection Law*, 33 COMPUT. L. & SEC. REV. 618, 619 (2017).

15. Christina Farr, *23andMe Founder Anne Wojcicki Is Leading a DNA Revolution by Going Directly to Consumers*, CNBC: DISRUPTOR, https://www.cnbc.com/2018/05/22/23andme-took-years-building-a-direct-to-consumer-health-business.html (May 22, 2018, 5:45 PM).

biological makeup of individuals, and it can reveal personal characteristics and susceptibility to a range of genetic conditions.[16]

More recently, biometric data gathering has gone a step further. In 2014, a company known as OpenBCI began offering a brain-computer interface (BCI) that measures electric activity through electrodes attached to a user's head.[17] It creates an electro-encephalogram (EEG) that is sent to a computer and then to a website for analysis.[18] Other companies soon followed with similar devices.[19] The EEGs, when coupled with other physiological measurements, can reveal intimate details of a user's thoughts and feelings.[20]

What happens to the health and biometric data these companies receive? That is largely up to the companies.[21] There are laws that protect many kinds of computerized data from disclosure without the subject's permission, but they leave glaring holes for data collected by companies that offer their

16. *Genetics vs. Genomics Fact Sheet*, NAT'L HUM. GENOME RSCH INST., https://www.genome.gov/about-genomics/fact-sheets/Genetics-vs-Genomics (Sept. 7, 2018). The term "genomic" refers to data on a person's entire complement of DNA and the term "genetic" refers to data on a specific gene or collection of genes. *Id.*; *see also Deoxyribonucleic Acid (DNA)*, NAT'L HUM. GENOME RSCH INST., https://www.genome.gov/genetics-glossary/Deoxyribonucleic-Acid (Mar. 4, 2023) ("Deoxyribonucleic acid (abbreviated DNA) is the molecule that carries genetic information for the development and functioning of an organism.").

17. Joel Murphy & Conor Russomanno, *OpenBCI: An Open Source Brain-Computer Interface for Makers*, KICKSTARTER, https://www.kickstarter.com/projects/openbci/openbci-an-open-source-brain-computer-interface-fo (Dec. 9, 2015).

18. Reuven Cohen, *New Open Source Platform Allows Anyone To Hack Brain Waves*, FORBES (Jan. 3, 2014, 11:35 AM), https://www.forbes.com/sites/reuvencohen/2014/01/03/new-open-source-platform-allows-anyone-to-hack-brain-waves/?sh=4b566ccc1b3f.

19. Jef Akst, *The Rise of BCI Enables Advances in Neuroscience*, THESCIENTIST (Oct. 1, 2020), https://www.the-scientist.com/bio-business/the-rise-of-bci-enables-advances-in-neuroscience-67995.

20. Nick Merrill, John Chuang & Coye Chesire, *Sensing is Believing: What People Think Biosensors Can Reveal About Thoughts and Feelings*, *in* DIS '19: PROCEEDINGS OF THE 2019 ON DESIGNING INTERACTIVE SYSTEMS CONFERENCE 413, 413–14 (2019).

21. *See Biometric Data and Privacy Laws (GDPR, CCPA/CPRA)*, THALES, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data (June 16, 2021) ("Despite the very particular character of such information, virtually no legal provisions in the world are specific to biometric data protection.").

services on a direct-to-consumer (DTC) basis.[22] For highly personal genetic and neurotechnology data, users are left vulnerable to unauthorized data sharing and disclosure that could have serious repercussions.[23]

The status of genetic information collected by DTC companies has revealed the shortcomings of existing laws and led to calls for greater privacy protections.[24] Those shortcomings apply equally to the emerging industry of brain data collection based on EEGs.[25] As the newer technology spreads, the issues surrounding genetic data offer a preview of issues and concerns that can be expected to emerge, but also of possible legal remedies.[26]

This Article describes the risks to consumers that collection of data by DTC biometric companies present and the lessons that genetic data collection may hold for neurotechnology. Part I describes the technologies, the risks of unauthorized disclosure of the data they collect, and the exceptional nature of the data and risks involved. Part II describes the evolution of the recognition of privacy as a fundamental right. Part III explains existing legal oversight mechanisms for data security and their shortcomings. Part IV describes the special status of DTC data. Part V presents proposals for legal reform. The Article ends

22. Sara Gerke & Chloe Reichel, *Perspectives on Data Privacy for Direct-to-Consumer Health Apps*, BILL OF HEALTH (Aug. 18, 2021), https://blog.petrieflom.law.harvard.edu/2021/08/18/data-privacy-direct-to-consumer-health-apps/; Max Freedman, *How Businesses Are Collecting Data (and What They're Doing with It)*, BUS. NEWS DAILY, https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (Feb. 21, 2023).

23. Hadley Leggett, *Risks of Sharing Personal Genetic Information Online Need More Study, Stanford Bioethicists Say*, STAN. MED. NEWS CTR. (June 4, 2009), https://med.stanford.edu/news/all-news/2009/06/risks-of-sharing-personal-genetic-information-online-need-more-study-stanford-bioethicists-say.html; *see also* Catherine Roberts, *Your Genetic Data Isn't Safe*, CONSUMER REPS. (July 23, 2020), https://www.consumerreports.org/health-privacy/your-genetic-data-isnt-safe-direct-to-consumer-genetic-testing-a1009742549/.

24. Mark Phillips, Fruzsina Molnár-Gábor, Jan O. Korbel, Adrian Thorogood, Yann Joly, Don Chalmers, David Townend & Bartha M. Knoppers, *Genomics: Data Sharing Needs an International Code of Conduct*, NATURE (Feb. 5, 2020), https://www.nature.com/articles/d41586-020-00082-9.

25. The Committee on Science and Law, *Are Your Thoughts Your Own?: "Neuroprivacy" and the Legal Implications of Brain Imaging*, 60 RECORD 407, 423–35 (2005).

26. *See id.* at 411–12.

with conclusions on the need to achieve a balance between privacy protection and medical innovation.

I. THE NATURE OF GENOMIC AND NEUROTECHNOLOGY DATA

Information about a person's genome reveals the blueprint for their physiological makeup, and information about their brain activity could reveal their innermost thoughts.[27] It is difficult to imagine any kinds of data that would be more personal. As a result, unauthorized disclosure could cause distinct kinds of harm. An understanding of the nature of these data helps to explain the risks should their confidentiality be compromised.

A. *Genomic Data Uses and Risks*

The genomes of all living things are comprised of strands of DNA wound around each other to form a double helix.[28] The DNA in those strands is comprised of arrangements of four bases—adenine, cytosine, guanine, and thymine—that are complimentary.[29] An adenine on one strand is always paired with a thymine on the other and a cytosine with a guanine.[30]

DNA of the human genome has about three billion base pairs that are arranged in twenty-three pairs of chromosomes located within the nucleus of every cell.[31] Individual genes that determine the activity of a cell can have as few as about 25,000 and as many as about 90,000 base pairs.[32] Once the sequence of

27. *Genomes at Work*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/dna-day/15-ways/genomes-at-work (Apr. 12, 2018).

28. *1953: DNA Double Helix*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/25520255/online-education-kit-1953-dna-double-helix (Apr. 23, 2013).

29. *Id.*

30. *Id.*

31. Sarah A. Bates, *Base Pair*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/genetics-glossary/Base-Pair (Apr. 11, 2023); Eric Green, *Genome*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/genetics-glossary/Genome (Apr. 11, 2023).

32. *See* Inês Lopes, Gulam Altab, Priyanka Raina & João Pedro de Magalhães, *Gene Size Matters: An Analysis of Gene Length in the Human Genome*, 12 FRONTIERS IN GENETICS, Feb. 2021, at 1, 4.

bases in a gene contained in an individual's genome has been identified, it can be recorded and stored as a series of letters representing each base (A, C, G, T).[33] It is a code with four possible elements at each position,[34] much as a computer code is a code with two possible elements, zero and one.[35]

As with computer code, genetic code can be stored indefinitely.[36] Unlike biological samples, it does not degrade over time, and unlike tracking data from a website or application, it does not change with an individual's behavior.[37] Moreover, unlike health data from a smartwatch or similar device, it does not reflect merely a point in time but rather aspects of an individual's composition that remain constant over the course of his or her entire life.[38]

Genomic data has a variety of applications. For tens of millions of people who voluntarily enter their information into

33. *Genetics Review*, NAT'L CTR. FOR BIOTECHNOLOGY INFO., https://www.ncbi.nlm.nih.gov/Class/MLACourse/Original8Hour/Genetics/basepair.html (Sept. 29, 1999).

34. *1953: DNA Double Helix*, *supra* note 28.

35. *Binary Code*, ENCYC. BRITANNICA, https://www.britannica.com/technology/binary-code (last visited Apr. 12, 2023).

36. *See* Danny Lewis, *These Glass Discs Can Store Data for Billions of Years*, SMITHSONIAN MAG. (Feb. 18, 2016), https://www.smithsonianmag.com/smart-news/these-glass-discs-can-store-data-billions-years-180958163/; Stephen Pritchard, *Indefinite Storage: What It Is and Why You Might Need It*, COMPUT. WKLY. (Nov. 24, 2022), https://www.computerweekly.com/feature/Indefinite-storage-What-it-is-and-why-you-might-need-it; *DNA of Every Baby Born in California Is Stored. Who Has Access to It?*, CBS NEWS (May 12, 2018, 11:49 PM), https://www.cbsnews.com/news/california-biobank-dna-babies-who-has-access/ (stating how a biobank with genomic information on every baby born in California can store data indefinitely).

37. *See* Anne-Marie Laberge, *Genetics and Public Health*, ATLAS OF GENETICS & CYTOGENETICS IN ONCOLOGY & HAEMATOLOGY, Nov. 2004, https://atlasgeneticsoncology.org/teaching/30053/genetics-and-public-health ("Genetic information is different from other types of personal information found in a medical chart. First, genetic information does not change over time: the presence of a mutation or a polymorphism in an individual is immutable.").

38. *Id.* While epigenetics changes can alter gene expression over time, the underlying genetic sequence remains constant. Harrison Wein, *DNA Changes Predict Longevity*, NAT'L INSTS. OF HEALTH (Oct. 18, 2016), https://www.nih.gov/news-events/nih-research-matters/dna-changes-predict-longevity; *see also What Does It Mean to Have a Genetic Predisposition to a Disease?*, NAT'L LIBR. OF MED.: MEDLINE PLUS, https://medlineplus.gov/genetics/understanding/mutationsanddisorders/predisposition/ (May 14, 2021) ("Although a person's genetic makeup cannot be altered, some lifestyle and environmental modifications (such as having more frequent disease screenings and maintaining a healthy weight) may be able to reduce disease risk in people with a genetic predisposition.").

the databases of DTC testing companies, the primary motivation is to satisfy curiosity about their ancestry.[39] These companies can match an individual's data with that of ethnic groups around the world to provide an estimate of the portion of their ancestry derived from different groups.[40] Law enforcement has used DTC databases to find suspects in criminal cases by identifying relatives.[41] Such efforts have identified suspects in several cold cases involving crimes that had been committed decades earlier.[42] Information about genetic vulnerabilities can guide individuals in choosing lifestyles that minimize health risks that are specific to them and to maximize opportunities for enhancement.[43]

39. *See* Yeyang Su, Heidi C. Howard & Pascal Borry, *Users' Motivations to Purchase Direct-to-Consumer Genome-Wide Testing: An Exploratory Study of Personal Studies*, 2 J. CMTY. GENETICS 135, 138, 141 (2011); Gena Philibert-Ortega, *Does Curiosity Drive Your Genealogy Research?*, LEGACY NEWS FAM. TREE (Nov. 4, 2022), https://news.legacyfamilytree.com/legacy_news/2022/11/curiosity-and-genealogy.html.

40. *What is Genetic Ancestry Testing?*, NAT'L LIBR. OF MED.: MEDLINEPLUS, https://medlineplus.gov/genetics/understanding/dtcgenetictesting/ancestrytesting/ (June 21, 2022).

41. *See, e.g.*, Lindsey Van Ness, *DNA Databases Are Boon to Police but Menace to Privacy, Critics Say*, PEW: STATELINE (Feb. 20, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/20/dna-databases-are-boon-to-police-but-menace-to-privacy-critics-say ("The man accused of being the Golden State Killer, Joseph James DeAngelo, was arrested after investigators uploaded crime-scene DNA to online genealogy database GEDmatch, matched it partially to his great-great-great-grandparents, built family trees of relatives and eventually traced it to him."); *see also* U.S. DEP'T OF JUST., USING DNA TO SOLVE COLD CASES: SPECIAL REPORT 9 (2002), https://www.ojp.gov/pdffiles1/nij/194197.pdf ("CODIS is a computer software program [used by law enforcement] that operates local, State, and national databases of DNA profiles from convicted offenders, unsolved crime scene evidence, and missing persons.").

42. *See* Van Ness, *supra* note 41.

43. *See* Theresa M. Marteau & Caryn Lerman, *Genetic Risk and Behavioural Change*, 322 BRIT. MED. J. 1056, 1057 ("Genetic risk information could both increase and decrease motivation to change behaviour."); NAT'L ACAD. OF SCIS., GENES, BEHAVIOR, AND THE SOCIAL ENVIRONMENT: MOVING BEYOND THE NATURE/NURTURE DEBATE 68–82 (Lyla M. Hernandez & Dan G. Blazer eds., 2006) (discussing how genetic, social, and behavioral factors influence an individual's risk of disease); *see also Genomics and Precision Health Topics*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/genomics/disease/genomic_diseases.htm (Feb. 10, 2022) ("Genomics and family health history play a role in many diseases such as cancer and heart disease. These diseases are partly the result of how your genes interact with your behaviors, such as your diet and physical activity, the environment, and other social factors."); *Genetic Testing*, CTRS. FOR DISEASE CONTROL & PREVENTION, https://www.cdc.gov/genomics/gtesting/

Perhaps most importantly, genomic data is being used to develop a new field of medicine in which treatments are personalized based on a patient's genetic makeup.[44] Precision medicine has wide potential application, but has so far been used mostly in oncology to diagnose the nature of a patient's cancer based on the genetics of the patient and the tumor.[45] Based on this information, clinicians can select medications that are most likely to be effective and to have the fewest adverse effects.[46]

However, collection and maintenance of the genetic information on which these applications rest present risks for those whose data are collected and stored.[47] Organizations that maintain genetic databases, other than those used for clinical care, keep the data they collect in anonymous form.[48] Nevertheless, recent research has demonstrated the possibility of deanonymizing them.[49] Using demographic data and information on individual subjects, researchers have been able to discover the identities of many of them and many of their relatives.[50] It is estimated that once a subject has been identified, relatives as distant as third cousins can also be identified, even those who never contributed genetic samples.[51] Researchers

genetic_testing.htm (June 24, 2022) (stating genetic testing can allow an individual to determine whether they need to make changes to their medical care or take preventative measures if an individual is more at risk of a certain disease).

44. *See* Geoffrey S. Ginsburg & Kathryn A. Phillips, *Precision Medicine: From Science to Value*, 37 HEALTH AFFS. J. 694, 694 (2018).

45. *Id.* at 695.

46. Allen D. Roses, *Pharmacogenetics*, 10 HUM. MOLECULAR GENETICS 2261, 2266 (2001).

47. *What are the Benefits and Risks of Direct-to-Consumer Genetic Testing?*, MEDLINEPLUS, https://medlineplus.gov/genetics/understanding/dtcgenetictesting/dtcrisksbenefits/ (June 21, 2022).

48. *See Can my DNA be Genotyped Anonymously?*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/202907890-Can-My-DNA-Be-Genotyped-Anonymously (last visited Apr. 12, 2023).

49. *See* Gina Kolata, *Your Data Were 'Anonymized'? These Scientists Can Still Identify You*, N.Y. TIMES (July 23, 2019), https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html.

50. Yaniv Erlich, Tal Shor, Itsik Pe'er, & Shai Carmi, *Identity Inference of Genomic Data Using Long-Range Familial Searches*, 362 SCI. 690–91 (2018).

51. *See id.* at 690.

believe that genetic databases can currently identify 60% of Americans of Northern European descent.[52]

Disclosure of an individual's genome can cause many kinds of harm. A genetic pattern associated with susceptibility to a debilitating condition, such as various forms of mental illness and early onset Alzheimer's disease, can cause embarrassment and social stigma.[53] Revelations regarding parentage and lineage can disturb family relationships.[54] Some ethnic groups may find discoveries about ancestral roots offensive to religious and cultural beliefs.[55] On a broader scale, genetic information tied to race and ethnicity can reinforce discredited beliefs about racial differences that have been used in the past to justify programs of eugenics.[56]

52. *See id.*

53. *See* Eric R. Rosin, Drew Blasco, Alexander R. Pilozzi, Lawrence H. Yang & Xudong Hang, *A Narrative Review of Alzheimer's Disease Stigma*, 78 J. ALZHEIMER'S DISEASE 515, 516 (2020).

54. *See* Blaine Bettinger, *A DNA Case Study: Revealing a Misattributed Parentage Event with DNA*, THE GENETIC GENEALOGIST (Mar. 13, 2017), https://thegeneticgenealogist.com/2017/03/13/a-dna-case-study-revealing-a-misattributed-parentage-event-with-dna/.

55. *See* Charles Petit, *Trying to Study Tribes While Respecting Their Cultures / Hopi Indian Geneticist Can See Both Sides*, SFGATE (Feb. 19,1998, 4:00 PM), https://www.sfgate.com/news/article/Trying-to-Study-Tribes-While-Respecting-Their-3012825.php. In 1990, researchers from Arizona State University began collecting genetic samples from members of the Havasupai tribe, who live near the Grand Canyon. Jeantine E. Lunshof & Ruth Chadwick, *Editorial: Genetic and Genomic Research—Changing Patterns of Accountability*, 18 ACCOUNTABILITY RSCH. 121, 126–27 (2011); Charles Pensabene, *A Canyon Full of Woes: The Havasupai Tribe Illustrates the Need for Cultural Competency in Genetic Research*, 7 ALB. GOV'T L. REV. 637, 639–40 (2014). Research subjects were told that the samples would be used for research on genetic correlates of type 2 diabetes. *See* Lunshof & Chadwick, *supra*; *see also* Pensabene, *supra*. However, the samples were subsequently used for research into other conditions, including schizophrenia, without the subjects' knowledge or consent. Lunshof & Chadwick, *supra*, at 127; Pensabene, *supra*, at 648. They were also used to study patterns of population migration, which produced findings that were at odds with the tribe's religious tradition. Lunshof & Chadwick, *supra*, at 127; *see also* Pensabene, *supra*, at 648. The tribe sued the University in 2004, and the suit was settled in 2010 for $700,000 distributed among forty-one members of the tribe and the return of the samples. Lunshof & Chadwick, *supra*, at 126; Pensabene, *supra*, at 640, 642.

56. *See* Ramin Skibba, *The Disturbing Resilience of Scientific Racism*, SMITHSONIAN MAG. (May 20, 2019), https://www.smithsonianmag.com/science-nature/disturbing-resilience-scientific-racism-180972243/.

An individual's genetic information could also become the basis for various forms of discrimination.[57] Insurance companies could use an individual's risk profile for genetically-based illnesses to exclude coverage or raise premiums for life, health, disability, and long-term care coverage.[58] Employers could use findings of genetic risks to exclude prospective workers who could add costs to their health care plans, miss workdays, or be less productive when illness strikes.[59] Landlords could avoid prospective tenants who might be more likely to become unemployed because of illness leading to difficulty in paying rent.[60] Long-term care facilities might avoid prospective residents who are prone to developing Alzheimer's disease or other debilitating conditions that require more intensive care.[61] Banks could reject mortgage applications from customers at risk for illnesses that could strain their ability to repay.[62]

For these reasons, threats to the privacy of individuals whose genomes are maintained in databases raise significant concerns.[63] Data that are stored safely and anonymously are nonetheless subject to the risk of unauthorized disclosure both through breaches and deliberate disclosure and as a result, to possible deanonymization.[64] Disclosure also presents a risk to

57. M.R. Natowicz, Jane K. Alper & Joseph S. Alper, *Genetic Discrimination and the Law*, 50 AM. J. HUM. GENETICS 465, 465 (1992); *see What is Genetic Discrimination?*, MEDLINEPLUS, https://medlineplus.gov/genetics/understanding/testing/discrimination/ (July 28, 2021).

58. Natowicz et al., *supra* note 57, at 466; *see What is Genetic Discrimination?*, *supra* note 57.

59. Natowicz et al., *supra* note 57, at 467.

60. Kaitlyn Dowling, *Genetic Discrimination in Housing and Lending: What's the Risk?*, BILL OF HEALTH (Nov. 15, 2019), https://blog.petrieflom.law.harvard.edu/2019/11/15/genetic-discrimination-in-housing-and-lending-whats-the-risk/.

61. *See* Elaine A. Lisko, *Genetic Information and Long-Term Care Insurance*, UNIV. OF HOUS. L. CTR.: HEALTH L. & POL'Y INST. (June 29, 1998), https://www.law.uh.edu/healthlaw/perspectives/Managed/980629LongTerm.html.

62. *See* Mark A. Rothstein & Laura Rothstein, *The Use of Genetic Information in Real Property Transactions*, 31 PROB. & PROP. 13, 13, 15 (2017).

63. *See* 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., May 9, 2019, at 1, 2.

64. *See, e.g.*, *OCR Concludes All-Time Record Year for HIPAA Enforcement with $3 Million Cottage Health Settlement*, U.S. DEP'T OF HEALTH & HUM. SERVS. (June 8, 2020),

relatives who do not even know that data linked to them has been collected.[65] Genetic data are opening the floodgates to a wealth of advances but must be handled with extreme care.

B. *Brain Data Uses and Risks*

For users of some forms of neurotechnology, inner thoughts are not as private as most people have assumed.[66] Recent advances in neuroscience enable scientists to construct pictures of brain activity that could reveal much about our thoughts and feelings.[67] As with genetic data, these advances open new possibilities for dramatic medical advances, but they also pose risks to those whose brain data are collected and stored by third parties.[68]

Brain data can be collected in two ways: invasively with electrodes placed in the brain itself, and externally with sensors placed on the head.[69] Invasive techniques are producing extraordinary medical advances in translating thoughts into actions.[70] Among other breakthroughs, researchers are developing techniques to enable patients suffering from paralysis to move artificial limbs and to spell words on computers by thinking the letters.[71] Another breakthrough has

https://www.hhs.gov/guidance/document/ocr-concludes-all-time-record-year-hipaa-enforcement-3-million-cottage-health-settlement.

65. *See* Hendricks-Sturrup & Lu, *supra* note 63, at 2.

66. *See* Brenda Kelley Kim, *Can an EEG Read Your Mind?*, LABROOTS (Apr. 4, 2018, 5:47 AM), https://www.labroots.com/trending/neuroscience/8445/eeg-read-mind.

67. *See id.*

68. *See* Hendricks-Sturrup & Lu, *supra* note 63, at 2.

69. Oliver Müller & Stefan Rotter, *Neurotechnology: Current Developments and Ethical Issues*, FRONTIERS SYS. NEUROSCIENCE, Dec. 13, 2017, at 1, 1.

70. *See Neurotechnologies: The Next Technology Frontier*, IEEE BRAIN, https://brain.ieee.org/topics/neurotechnologies-the-next-technology-frontier/ (last visited Apr. 12, 2023).

71. *See, e.g.*, *New Device Allows Brain to Bypass Spinal Cord and Move Paralyzed Limbs*, NEUROSCIENCE NEWS (June 24, 2014), https://neurosciencenews.com/paralysis-neurobridge-neural-bypass-movement-1131/ (detailing the Neurobridge technology, an invasive technique, that combines technology to decode brain activity with a "muscle stimulation sleeve" that translates brain signals and "transmits [them] to the paralyzed limb"); Jon Hamilton, *Man Who Is Paralyzed Communicates by Imagining Handwriting*, NPR (May 12, 2021, 12:03 PM), https://www.npr.org/sections/health-shots/2021/05/12/996141182/paralyzed-man-

helped patients control shaking from Parkinson's disease and manage symptoms of other debilitating conditions.[72] However, invasive technologies can also permit researchers to learn details of brain function and the very process of thinking.[73]

Invasive brain procedures are conducted as part of patient care and research on patients with serious medical conditions.[74] In contrast, external measurements of brain activity are available to almost anyone.[75] They can be used not only for the treatment of neurological disorders and research but also for anyone seeking to learn more about the functioning of their brain.[76] For these people, DTC companies offer external brain-computer interfaces with electrodes that attach to the outside of the head and transmit the impulses to their computer from the comfort of their home.[77] In the collection of data, the business of providing BCIs has much in common with DTC genetic testing companies that enable customers to simply collect saliva and send it for analysis.[78]

communicates-by-imagining-handwriting (describing an invasive tool "that turns thoughts into text").

72. *See* Müller & Rotter, *supra* note 69, at 2.

73. *See Neurotechnology, How to Reveal the Secrets of the Human Brain?*, IBERDROLA, https://www.iberdrola.com/innovation/neurotechnology (last visited Mar. 5, 2023); Stephen Rainey, Stéphanie Martin, Andy Christen, Pierre Mégevand, & Eric Fourneret, *Brain Recording, Mind-Reading, and Neurotechnology: Ethical Issues from Consumer Devices to Brain-Based Speech Decoding*, 26 SCI. & ENG. ETHICS 2295, 2297–98 (2020).

74. *See* Kelly Servick, *Window of Opportunity*, 375 SCI. 256, 257 (2022).

75. *See, e.g.*, EMOTIV, https://www.emotiv.com/ (last visited Apr. 12, 2023) (selling wireless EEG devices & software); ZETO, https://zeto-inc.com/ (last visited Apr. 12, 2023) (selling an EEG monitoring device); STRATUS, https://stratusneuro.com/ (last visited Apr. 12, 2023) (offering in-home testing and monitoring devices).

76. *See, e.g.*, Akriti Parida, *The Rise of Brain Computer Interfaces and the Future of Marketing*, FUTURE MKTG. INST. (Sept. 8, 2020), https://futureofmarketinginstitute.com/the-rise-of-brain-computer-interfaces-and-the-future-of-marketing/; P. Brunner, L. Bianchi, C. Guger, F. Cincotti & G. Schalk, *Current Trends in Hardware and Software for Brain-Computer Interfaces (BCIs)*, J. NEURAL ENG'G, Mar. 24, 2011, at 1, 3.

77. *See, e.g.*, EMOTIV, *supra* note 75 (offering "portable EEG technology . . . to gain valuable insights into the human brain"); *see also* ZETO, *supra* note 75 (offering "EEG equipment with live remote monitoring and reading services"); STRATUS, *supra* note 75 (providing "at-home video EEG tests [that] are equally effective and [one-third] the cost of . . . inpatient test[s]").

78. *See* Brunner et al., *supra* note 76, at 3; *What Is Direct-to-Consumer Genetic Testing?*, MEDLINEPLUS, https://medlineplus.gov/genetics/understanding/dtcgenetictesting/directtoconsumer/ (June 21, 2022).

The applications of external brain monitoring are not as dramatic as those of invasive implants, but they are nevertheless substantial.[79] The data this technology produces can be used to diagnose neurological diseases, such as epilepsy and traumatic brain injury.[80] External brain monitoring can also form the basis for therapies that use feedback to train patients to mitigate symptoms.[81] Feedback from brain data can also help patients with emotional disorders such as depression and anxiety.[82] For many people without major disorders, brain data may help to improve mental functioning and satisfy curiosity about mental activity.[83]

Beyond health care and wellness, brain data can be used in a number of other settings.[84] These include educational settings to improve memory and workplace settings to improve job performance.[85] Brain data can also be used for performance enhancement in areas such as the military and sports,[86] and in law enforcement settings, for example, to assess the veracity of memories of witnesses to crimes.[87]

79. *See* M.F. Mridha, Sujoy Chandra Das, Muhammad Mohsin Kabir, Aklima Akter Lima, Md. Rashedul Islam & Yutaka Watanobe, *Brain-Computer Interface: Advancement and Challenges*, 21 SENSORS 1, 5 (2021).

80. *See id.*

81. *See NeuroTech Applications*, NEUROTECHEDU, https://neurotechx.github.io/neurotechedu/applications.html (last visited Apr. 12, 2023).

82. *See id.*

83. *See Consumer EEG, Mental and Emotional States, Privacy and the Brain (2018-2019)*, DUKE UNIV.: BASS CONNECTIONS, https://bassconnections.duke.edu/project-teams/consumer-eeg-mental-and-emotional-states-privacy-and-brain-2018-2019 (last visited Apr. 12, 2023).

84. *See Neurotechnologies: The Next Technology Frontier*, *supra* note 70.

85. *See id.*

86. *See generally* Rizki Edmi Edison, *Application of Neuroimaging Technology in Military*, 7 JURNAL PERTAHANAN 430 (2021) (analyzing "potential uses of neuroimaging technology in the military"); Elaine R. Peskind, David Brody, Ibolja Cernak, Ann McKee & Robert L. Ruff, *Military- and Sports-Related Mild Traumatic Brain Injury: Clinical Presentation, Management, and Long-Term Consequences*, 74 J. CLINICAL PSYCHIATRY 180 (2013) (discussing "the effects of military-related and sports-related [traumatic brain injuries], long-term consequences, management, and prevention").

87. *See* Irina A. Filipova, *Neurotechnologies in Law and Law Enforcement: Past, Present, and Future*, 6 L. ENF'T REV. 32, 36–37 (2022); Alla Katsnelson, *Crime: Does Brain Scan Evidence Work?*, UNESCO, https://en.unesco.org/courier/2022-1/crime-does-brain-scan-evidence-work (last visited Apr. 17, 2023).

The data for these applications take the form of EEG readings reflecting patterns of electrical activity in different parts of the brain while electrodes are attached.[88] The readings can be displayed as graphs and the underlying data for the graphs can be stored as easily as any other form of information as computer code.[89] As with genetic sequences, once data are stored, they can be retained indefinitely.[90] However, storage of brain data is somewhat more complex, since the characteristics they reveal are not immutable and represent only one point in time.

At-home collection of brain data is also similar to genetic data collection in that both kinds of data are easy for consumers to provide.[91] Many commercial BCI interfaces only require that the user wear a cap similar to a bathing cap or a headset and connect it to a computer.[92] Algorithms contained in software on the computer or residing online provide the analysis.[93] The DTC brain data industry is newer than the DTC genomic data industry, but it is growing rapidly.[94]

88. *See* LESTER INGBER, STATISTICAL MECHANICS OF NEOCORTICAL INTERACTIONS: MULTIPLE SCALES OF EEG 1–5 (1993), https://www.ingber.com/smni96_eeg.pdf.

89. *See* Yannick Roy, Hubert Banville, Isabela Albuquerque, Alexandre Gramfort, Tiago H. Falk & Jocelyn Faubert, *Deep Learning-Based Electroencephalography Analysis: A Systematic Review*, 16 J. NEURAL ENG'G 1, 1, 4 (2019); *see also The Introductory Guide to EEG (Electroencephalography)*, EMOTIV, https://www.emotiv.com/eeg-guide/ (last visited Apr. 17, 2023) (explaining how EEG results are transmitted and stored).

90. *See, e.g.*, Danny Lewis, *These Glass Discs Can Store Data for Billions of Years*, SMITHSONIAN MAG. (Feb. 18, 2016), https://www.smithsonianmag.com/smart-news/these-glass-discs-can-store-data-billions-years-180958163/; *see also* Stephen Pritchard, *Indefinite Storage: What It Is and Why You Might Need It*, COMPUT. WKLY. (Nov. 24, 2022), https://www.computerweekly.com/feature/Indefinite-storage-What-it-is-and-why-you-might-need-it.

91. *See* EMOTIV, *supra* note 75 (describing the development of "the world's largest anonymous EEG database" that enables "a seamless way to create meaningful measurements"); *What Is Direct-to-Consumer Genetic Testing?*, *supra* note 78 ("The number of companies providing direct-to-consumer genetic testing is growing, along with the range of health information provided by these tests.").

92. *See, e.g.*, *Emotiv EPOC Flex*, EMOTIV, https://www.emotiv.com/epoc-flex/ (last visited Apr. 17, 2023) (advertising variable cap sizes for optimal fitting).

93. *The Science Behind Our Technology*, EMOTIV, https://www.emotiv.com/our-technology/ (last visited Apr. 17, 2023).

94. *See* Henry T. Greely, *The Future of DTC Genomics and the Law*, 48 J.L. MED. ETHICS 151, 151 (2020) ("November 19, 2007 can be called the effective beginning of DTC genomics, although a few firms offered some services earlier."); Jef Akst, *The Rise of BCI Enables Advances in Neuroscience*, THESCIENTIST (Oct. 1, 2020), https://www.the-scientist.com/bio-business/the-rise-

Ease of use and the growing reach of data collection raise similar privacy concerns to those raised by genomic data collection.[95] Revelation of private thoughts could lead to embarrassment.[96] Information on others whom the subject knows, not just relatives, could be exposed.[97] Information that reveals personal characteristics could lead to discrimination in a range of contexts, including insurance, employment, housing, and finance.[98]

A subject may be entirely unaware of the thoughts that are being monitored, as some researchers claim that they can uncover unconscious thoughts.[99] An experiment conducted by researchers at the University of Washington used the video game Flappy Whale to probe for reactions to stimuli presented subliminally.[100] The game became progressively more difficult,

of-bci-enables-advances-in-neuroscience-67995 (stating how in 2014, "[t]he consumer [brain-computer interface (BCI)] industry was just beginning to blossom"); Contrive Datum Insights Pvt Ltd, *Brain Computer Interface Market Is Projected To Reach US$ 9.31 Billion by 2030, at a CAGR of 16.26% During the Forecast Period 2022-2030*, YAHOO (Jan. 25, 2023), https://www.yahoo.com/now/brain-computer-interface-market-projected-050000948.html?guccounter=1 ("The global Brain Computer Interface Market was valued at USD 2.79 Billion in 2022 and is projected to reach USD 9.31 Billion by 2030, growing at a CAGR of 16.26% from 2023 to 2030.").

95. *Compare* Swish Goswami, *The Rising Concern Around Consumer Data and Privacy*, FORBES (Dec. 14, 2020, 7:40 AM), https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/?sh=209e8467487e, *with Privacy in Genomics*, NAT'L HUM. GENOME RSCH. INST., https://www.genome.gov/about-genomics/policy-issues/Privacy (Apr. 27, 2021) (comparing the concerns of company data collection with similar concerns related to genetic data collection).

96. *See, e.g.*, *GSP Data Use Agreement*, USC STEVENS NEUROIMAGING & INFORMATICS INST.: IMAGE & DATA ARCHIVE, https://ida.loni.usc.edu/collaboration/access/appLicense.jsp (last visited Apr. 17, 2023) (warning, as part of a genomics study, that "some data elements might harm or embarrass individuals if they were inadvertently disclosed.").

97. *Cf.* 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, 5 (2019) (explaining how the collection of sensitive genetic information leads to implications about certain groups that can result in "major social and economic consequences.").

98. *See* Samantha Lai & Brooke Tanner, *Examining the Intersection of Data Privacy and Civil Rights*, BROOKINGS (July 18, 2022), https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights/.

99. *NeuroTech Applications*, NEUROTECHEDU, https://neurotechx.github.io/neurotechedu/applications.html (last visited Apr. 17, 2023).

100. *See* Tamara Bonaci, Univ. of Wash., Brains Can Be Hacked. Why Should You Care? at USENIX Enigma 2017 (Jan. 31, 2017), https://www.usenix.org/conference/enigma2017/

requiring greater levels of concentration as a subject progressed.[101] Subjects wore external monitors that captured brain activity as they played.[102] Interspersed among the game's images were images of corporate logos that were displayed for a few milliseconds, durations too short for subjects to be consciously aware of them.[103] The electrical activity detected by the monitors revealed reactions to the logos, and presumably to the corporations involved.[104] The researchers hypothesized that the same technique could be used to probe for such private information as financial status, religious beliefs, political leanings, medical conditions, and personal prejudices.[105] The researchers did not attempt to replicate the experiment, and it is unknown whether anyone else has tried to.[106] However, the researchers were able to establish that this technique is feasible.[107]

An even more concerning possibility, and one that is unique to the collection of brain data, is the potential for psychological manipulation.[108] An extreme scenario, although one that may be feasible in the not-too-distant future, is one in which thoughts

conference-program/presentation/bonaci [hereinafter Brains Can Be Hacked. Why Should You Care? at USENIX Enigma 2017]; Tamara Bonaci, Security and Privacy of Biomedical Cyber-Physical Systems 27 (2015) (Ph.D. dissertation, University of Washington) (on file with ResearchWorks Archive, University of Washington) [hereinafter Security and Privacy of Biomedical Cyber-Physical Systems].

101. *See Brains Can Be Hacked. Why Should You Care?*, *supra* note 100; Security and Privacy of Biomedical Cyber-Physical Systems, *supra* note 100, at 30.

102. *See* Security and Privacy of Biomedical Cyber-Physical Systems, *supra* note 100, at 26.

103. *See id.* at 28–29.

104. *See id.* at 36.

105. *Id.* at 3; *see also* MARYNA KAPITONOVA, PHILLIPP KELLMEYER, SIMON VOGT & TONIO BALL, A FRAMEWORK FOR PRESERVING PRIVACY AND CYBERSECURITY IN BRAIN-COMPUTER INTERFACING APPLICATIONS 16 (2022), https://arxiv.org/pdf/2209.09653.pdf (stating how another study indicated brain stimuli devices would be used to extract private information such as "PIN codes, bank information, the month of birth, familiar faces, and geographical locations of the user").

106. KAPITONOVA ET AL., *supra* note 103, at 16–17.

107. Security and Privacy of Biomedical Cyber-Physical Systems, *supra* note 100, at 36–37; KAPITONOVA ET AL., *supra* note 105, at 16–17.

108. Marcello Ienca & Roberto Andorno, *Towards New Human Rights in the Age of Neuroscience and Neurotechnology*, 13 LIFE SCIS., SOC'Y & POL'Y 1, 2 (2017).

are implanted with internally placed electrodes.[109] A more immediate possibility is that feedback protocols using external electrodes could encourage specific thoughts and feelings.[110] If one of these scenarios were to come to fruition, the hazards of brain data collection would be elevated beyond concerns for privacy to concerns for freedom of thought,[111] arguably the most important freedom there is.

C. *Genomic and Brain Data Exceptionalism*

The characteristics of genomic and brain data are distinct from those of other kinds of personal information, including biometric data.[112] Both kinds of data are different from biological samples in that, once they are stored in computerized form, they do not degrade and they last indefinitely.[113] They are different from other forms of biometric data in that they reveal highly personal facts about a person that can cause extreme social and psychological consequences if disclosed.[114] Genomic and brain data also differ from other kinds of personal data in that they can reveal sensitive details not only about the person involved but also about others who have never consented to the data's collection.[115] Identification of third parties is also possible with many smart phone apps and websites that can access a user's contacts, but the potential to gain personal information about them surreptitiously is not as great.[116] The user knows

109. *See id.* at 21.

110. *See, e.g.*, Christof Koch, *Electrodes that Stimulate the Brain Reveal the Roots of Conscious Experience*, SCI. AM. (June 1, 2021), https://www.scientificamerican.com/article/electrodes-that-stimulate-the-brain-reveal-the-roots-of-conscious-experience/.

111. Ienca & Adorno, *supra* note 108, at 1.

112. *See* Deborah Hellman, *What Makes Genetic Discrimination Exceptional?*, 29 AM. J.L. & MED. 77, 82–83 (2003). The notion that genetic data are exceptional has been controversial. However, the view that their benefits and risks are distinctive has seen growing acceptance. *See, e.g.*, *id.*

113. *See, e.g.*, Lewis, *supra* note 36; *see also* Pritchard, *supra* note 36.

114. *See* Marie Oestreich, Dingfan Chen, Joachim L. Schultze, Mario Fritz & Matthias Becker, *Privacy Considerations for Sharing Genomics Data*, 20 EXCLI J. 1243, 1247–50 (2021).

115. *See id.* at 1247; Erlich et al., *supra* note 50, at 690.

116. *See, e.g.*, *Control Access to Information in Apps on iPhone*, APPLE, https://support.

who these people are, and the data do not usually include sensitive biometric information.[117] Genomic and neurotechnology data even allow identification of people the user does not know and without the user's knowledge that it is possible to identify them.[118]

Genomic data have the additional distinctive feature of being immutable.[119] Unlike performance information from a physiological monitoring device or a record of online activity, the data's subject can never change the characteristics that are revealed.[120] Brain data, by revealing the underlying process of thinking, have the additional distinctive feature of enabling behavioral manipulation to an extent permitted by no other form of information technology.[121]

While these exceptional forms of data have permitted the creation of exceptional applications that are tremendously beneficial to millions, they also present exceptional threats to privacy.[122] Those threats are widespread because these data are collected on large numbers of people by DTC companies.[123] They call for a new level of vigilance and new kinds of legal

apple.com/guide/iphone/control-access-to-information-in-apps-iph251e92810/ios (last visited Apr. 17, 2023) (explaining that iPhone users have control over whether third-party apps can access information contained in other apps on the user's phone because "[t]he first time an app wants to use information from another app, you receive a request with an explanation," which the user can grant or deny).

117. *See id*.

118. *See* Erlich et al., *supra* note 50, at 690.

119. Samuel Greengard, *Is Genomic Privacy Possible?*, COMMC'NS OF THE ASS'N FOR COMPUT. MACH. (Aug. 30, 2018), https://cacm.acm.org/news/230750-is-genomic-privacy-possible/fulltext.

120. Security and Privacy of Biomedical Cyber-Physical Systems, *supra* note 100, at 36–37 (finding that electrical activity produced in response to subliminal stimuli can be detected and the same process can likely be "used to expose private and sensitive information about a user").

121. *See* Liam Drew, *The Ethics of Brain–Computer Interfaces*, NATURE (July 24, 2019), https://www.nature.com/articles/d41586-019-02214-2.

122. *See id*.

123. *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/2019/02/11/103446/more-than-26-million-people-have-taken-an-at-home-ancestry-test/.

protections, that, as discussed in section IV below, are largely lacking.[124]

II. THE NATURE OF THE INTEREST IN PRIVACY

Legal recognition of a right to privacy dates back only as far as the beginning of the twentieth century.[125] With the advance of technologies that are capable of capturing ever greater amounts of personal information, the importance of a right to privacy has grown steadily since then.[126] Application of the right presents particular challenges when the collection of personal information can be used to develop technologies that benefit large numbers of people.[127] A review of the history of the right illustrates the way those challenges have become more difficult to resolve with the collection of highly sensitive genomic and brain data.

A. *Development of the Law and Ethics of Privacy*

The privacy of one's personal information, once considered a preference or luxury, is now widely seen as a fundamental human right.[128] The origin of the legal and ethical construct of a right to privacy in the United States can be traced to an article written by Samuel Warren and future Supreme Court justice Louis Brandeis in 1890.[129] Such a right was not mentioned in the Constitution and had not been widely considered as a fundamental right,[130] but Warren and Brandeis argued that

124. *See* discussion *infra* Part IV.

125. *See* discussion *infra* Section II.A.

126. *See* Hsiao-Ying Huang & Masooda Bashir, *Is Privacy a Human Right? An Empirical Examination in a Global Context*, *in* THIRTEENTH ANNUAL CONFERENCE ON PRIVACY, SECURITY & TRUST (PST) 77, 77 (2015); *see also* discussion *infra* Section II.A.

127. *See* discussion *infra* Section II.C.

128. *See* Shivnath Tripathi, Right to Privacy as a Fundamental Right: Extent and Limitations 3 (June 17, 2017) (unpublished work), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2273074.

129. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

130. *See* TRIPATHI, *supra* note 128, at 1–2.

because of developments in science and business, new restrictions on the unauthorized disclosure of personal information were needed.[131] In particular, they pointed to rapidly developed photographs and their distribution in newspapers as creating new risks for individuals, stating:

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right "to be let alone." Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops."[132]

International recognition of the right did not come for another sixty years.[133] The Universal Declaration of Human Rights, issued in 1948, declared in Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[134]

However, wider recognition of the right to privacy came slowly and haphazardly.[135] It was incorporated in the European

131. Warren & Brandeis, *supra* note 129, at 195–96. It has been argued that Warren and Brandeis responded to the needs of the society in which they lived and provided the catalyst for developments in privacy law in the late twentieth and early twenty-first century. Benjamin E. Bratman, *Brandeis and Warren's* The Right to Privacy *and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623, 650–51 (2002). Their call for greater protection "ultimately blossomed into all that we know today as 'privacy law.'" *Id.* at 650.

132. Warren & Brandeis, *supra* note 129, at 195.

133. *See* Oliver Diggelmann & Maria Nicole Cleis, *How the Right to Privacy Became a Human Right*, 14 HUM. RTS. L. REV. 441, 443 (2014).

134. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

135. *See* Diggelmann & Cleis, *supra* note 133, at 457.

Convention on Human Rights in 1953,[136] and the International Covenant on Civil and Political Rights in 1976,[137] but, in the view of some authors, the right to privacy was considered more as an afterthought than as a clear commitment.[138] When the first declarations were drafted during the years after World War II, there was no conscious decision to create an essential privacy guarantee.[139] In the words of one author, "[t]he right's potential was dramatically underestimated at the time of its creation."[140]

Today, the right to privacy is recognized in the constitutions of many nations,[141] and laws protecting privacy are in effect in 120 countries.[142] Although it is not mentioned in the United States Constitution, it has been recognized in a line of Supreme Court cases as a fundamental right.[143] These include *Griswold v. Connecticut*, which struck down laws prohibiting the use of contraceptives by married couples,[144] *Eisenstadt v. Baird*, which struck down similar laws regarding unmarried couples,[145] *Roe v. Wade*, which struck down restrictions on abortion[146] (although it has recently been overruled[147]), and *Lawrence v. Texas*, which struck down laws outlawing consensual sexual relations between same-sex couples.[148] The tort of invasion of privacy is

136. European Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, art. 8, 213 U.N.T.S. 221 (entered into force Sept. 3, 1953), as amended by Protocols Nos. 11, 14, and 15 (entered into force Nov. 1, 1998, June 1, 2010, and Aug. 1, 2021 respectively) [hereinafter European Convention on Human Rights]. "Everyone has the right to respect for his private and family life, his home and his correspondence." *Id.*

137. G.A. Res. 2200A (XXI), art. 17 (Dec. 16, 1966).

138. *See* Diggelmann & Cleis, *supra* note 133, at 441.

139. *Id.* at 441–42.

140. *Id.* at 441.

141. James Griffin, *The Human Right to Privacy*, 44 SAN DIEGO L. REV. 697, 703–04 (2007).

142. Giovanni Buttarelli, *Privacy Matters: Updating Human Rights for the Digital Society*, 7 HEALTH & TECH. 325, 326 (2017).

143. *See infra* notes 144–48; *see also Students: Your Right to Privacy*, ACLU, https://www.aclu.org/other/students-your-right-privacy (last visited Apr. 17, 2023).

144. Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965).

145. Eisenstadt v. Baird, 405 U.S. 438, 453 (1972).

146. Roe v. Wade, 410 U.S. 113, 153–54, 164–65 (1973), *overruled by* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2242 (2022).

147. *Dobbs*, 142 S. Ct. at 2242.

148. Lawrence v. Texas, 539 U.S. 558, 578 (2003).

recognized in the laws of many states, although based on different authorities, including statutes, common law, and natural law.[149]

The commitment to privacy as a fundamental right has taken on growing prominence in the last few decades as new technologies have created new threats to the right "to be let alone."[150] In Warren and Brandeis' day, the capacity of newspapers to disseminate photographs of individuals that contained information they would prefer not to be disclosed sent up an alarm.[151] However, the data included in newsprint usually faded from public view as the next day's newspaper arrived.[152] Moreover, it was not maintained in large centralized databases or likely to be systematically merged with other personal information.[153]

Commercial data collection and aggregation first appeared in the middle of the twentieth century and soon grew in capability and application.[154] Credit cards became ubiquitous forms of payment in the 1950s and 1960s, giving the companies that issued the cards information on the purchasing activities of millions of people.[155] In the 1980s, some retailers began issuing loyalty cards that offered discounts, while collecting

149. *Common Law Right to Privacy*, USLEGAL, https://privacy.uslegal.com/common-law-right-to-privacy/ (last visited Mar. 5, 2023).

150. *See* Warren & Brandeis, *supra* note 129 (discussing "the right 'to be let alone,'" as characterized by Judge Cooley, during the height of newspapers and new mechanical devices); Buttarelli, *supra* note 142, at 327 (discussing the evolution of technology and the consequential threats to personal information).

151. *See* Warren & Brandeis, *supra* note 129, at 195–96.

152. *See* Buttarelli, *supra* note 142, at 327 (explaining that before Internet-enabled technologies developed, personal information was only available through physical means and was much more difficult to access).

153. *Id.* (describing how Internet enabled technologies changed the way information is communicated, shared, and stored).

154. *See* Andres Phillips, *A History and Timeline of Big Data*, TECHTARGET (Apr. 1, 2021), https://www.techtarget.com/whatis/feature/A-history-and-timeline-of-big-data.

155. *See Charge It*, NAT'L MUSEUM OF AM. HIST., https://americanhistory.si.edu/american-enterprise-exhibition/consumer-era/charge-it (last visited Apr. 17, 2023); *see also* Burt Helm, *Credit Card Companies Are Tracking Shoppers Like Never Before: Inside the Next Phase of Surveillance Capitalism*, FAST CO. (May 12, 2020), https://www.fastcompany.com/90490923/credit-card-companies-are-tracking-shoppers-like-never-before-inside-the-next-phase-of-surveillance-capitalism (discussing the extent of credit card data collection and its value).

information on what customers bought.[156] With the opening of the internet to commercial transactions in the 1990s,[157] individual behavior, interests, and preferences could be tracked, stored, and combined with other data by recording web searches, browsing history, and social media postings.[158] In recent years, technological advancements have enabled commercial enterprises to gather personal information through personal assistants, such as Amazon's Alexa and Apple's Siri, appliances, such as robotic vacuum cleaners, and door monitors, such as Doorbell and Ring.[159]

This information is routinely shared with entities known as data aggregators that combine data on individuals from multiple sources.[160] Information on a range of activities permits more precise targeting of advertisements and other kinds of messaging.[161] The addition of biometric data substantially expands the applications that could potentially exist.[162] To that

156. *See* Nada Elnahla & Leighann C. Neilson, *The History of Retail Loyalty Programs in North America*, 20 MKTG. AND SOC. CHANGE: MAKING HIST. AND CULTURE, 92, 94 (2021); Vilius Petkauskas, *Loyalty for Data: What Do Retailers Know About You?*, CYBERNEWS, https://cybernews.com/privacy/loyalty-for-data-what-do-retailers-know-about-you/ (Sept. 28, 2021); *What Type of Information Do Loyalty Cards Collect?*, AZPIRAL, https://www.azpiral.com/what-type-of-information-do-loyalty-cards-collect/ (last visited Apr. 17, 2023).

157. *See* Peter H. Lewis, *Attention Shoppers: Internet Is Open*, N.Y. TIMES (Aug. 12, 1994), https://www.nytimes.com/1994/08/12/business/attention-shoppers-internet-is-open.html (describing the first retail transaction on the Internet).

158. *See Internet Safety.Understanding Browser Tracking*, GCFGLOBAL, https://edu.gcfglobal.org/en/internetsafety/understanding-browser-tracking/1/ (last visited Apr. 17, 2023) (describing how online stores, such as Amazon & eBay track and store browsing history).

159. *See* Erika Rawes, *What Exactly Is the Internet of Things?*, DIGIT. TRENDS (Jan. 28, 2020), https://www.digitaltrends.com/home/what-is-the-internet-of-things/; Matt Burgess, *All the Data Amazon's Ring Cameras Collect About You*, WIRED (Aug. 5, 2022, 7:00 AM), https://www.wired.com/story/ring-doorbell-camera-amazon-privacy/.

160. *See* DAVID LOSHIN, BUSINESS INTELLIGENCE: THE SAVVY MANAGER'S GUIDE 295 (Andrea Dierna & Robyn Day eds., 2d ed. 2013).

161. *See* Spandana Singh, *The Role of Data in the Targeted Advertising Industry*, NEW AM., https://www.newamerica.org/oti/reports/special-delivery/the-role-of-data-in-the-targeted-advertising-industry/ (Feb. 18, 2020) (discussing web tracking, location tracking, cross-device tracking, & browser fingerprinting); Avi Goldfarb & Catherine Tucker, *Online Display Advertising: Targeting and Obtrusiveness*, 30 MKTG. SCI. 389, 389 (2011) (studying the effectiveness of targeted ads, obtrusive ads, and ads that combined the two techniques).

162. *See* Dave Gurney, *The Rise of Biometrics in Marketing*, ALCHEMETRICS (July 3, 2019), www.alchemetrics-uk.com/rise-of-biometrics-in-marketing/ [http://web.archive.org/web/2021

end, Apple has developed software that attaches to online medical records maintained by health systems and tracks appointments and questions to clinicians.[163] The addition of genomic and brain data, arguably the most personal kinds of data, brings the potential for intrusiveness to a new level.

With such technological developments in monitoring individuals, Warren and Brandeis' warning that harm could be caused by intrusions into personal aspects of people's lives takes on new urgency.[164] They could hardly have imagined the progression from unauthorized newspaper photographs to elements of the biological composition of individuals and their private thoughts. After its haphazard evolution in the late twentieth century, the fundamental human right of privacy has become a vital concern.

B. *Monetary Value of Data*

Although American law has recognized the importance of individual privacy for more than a century,[165] personal data is used by an ever-growing array of American business.[166] Personal data today has considerable value that derives from companies' abilities to provide micro-targeted advertisements

0926211536/https://www.alchemetrics-uk.com/rise-of-biometrics-in-marketing/].

163. *See Apple Announces Effortless Solution Bringing Health Records to iPhone*, APPLE, https://www.apple.com/newsroom/2018/01/apple-announces-effortless-solution-bringing-health-records-to-iPhone/ (Jan. 24, 2018) (announcing an update on Apple products that allows health records from participating medical institutions to be automatically uploaded to user's Health app); *see also* Todd Feathers, Simon Fondrie-Teitler, Angie Waller & Surya Mattu, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites (June 16, 2022, 12:46 PM) (describing Meta Pixel, "[a] tracking tool installed on many hospitals' websites [that] has been collecting patients' sensitive health information—including details about their medical conditions, prescriptions, and doctor's appointments —and sending it to Facebook").

164. *See* Warren & Brandeis, *supra* note 129, at 195–96 (providing a warning of the harm involved in the rise of gossip in newspapers as a trade).

165. *See supra* notes 144–48 and accompanying text; *see also History of Privacy Timeline*, UNIV. OF MICH.: INFO. & TECH. SERVS., https://safecomputing.umich.edu/privacy/history-of-privacy-timeline (last visited Apr. 17, 2023).

166. Paulius Jurcys, *What Is the Value of Your Data?*, TOWARDS DATA SCI. (Sept. 5, 2019), https://towardsdatascience.com/what-is-the-value-of-your-data-9341cd019b4d.

to individuals.[167] Collection and sale of this information generated an estimated $108.6 billion in revenue for companies in 2018 with profits from the information estimated at $56.5 billion.[168] By one calculation, internet companies such as Google and Facebook earned at least $202 per American user in 2018.[169]

Much has been written about the monetary value of data to companies that perform analytics using user data.[170] By one estimate, basic demographic data on an individual, such as age, gender, and location, are worth only $0.0005 per person, which translates to $500 dollars per million people.[171] However, more sensitive information, such as data containing financial details or health information, is worth more.[172] Companies that aggregate data sell information on thousands of people on a regular basis, so small sums for each bit of information can add up.[173] The average value of an active user's data to Facebook has been estimated at about two dollars per month.[174] In the third quarter of 2022, Facebook had about three billion users, making its data an extremely valuable asset.[175] The company used this

167. *See* Eric Broda, *Our Personal Data Is a Lot More Valuable Than We Can Imagine*, MEDIUM (July 19, 2019), https://medium.com/swlh/our-personal-data-is-a-lot-more-valuable-than-we-can-imagine-60af3b920da0; *see also* Max Freedman, *How Businesses Are Collecting Data (and What They're Doing with It)*, BUS. NEWS DAILY (Nov. 21, 2022), https://www.businessnewsdaily.com/10625-businesses-collecting-data.html (Feb. 21, 2023).

168. Robert J. Shapiro, *What Your Data Is Really Worth to Facebook*, WASH. MONTHLY (July 12, 2019), https://washingtonmonthly.com/2019/07/12/what-your-data-is-really-worth-to-facebook/.

169. *Id.*

170. *See, e.g.*, Yaron Cohen, *Understanding the Monetary Value of Data*, 7 DATA (Mar. 26, 2020), https://7wdata.be/analytics/understanding-the-monetary-value-of-data/ (listing ways for companies to understand the monetary value of their data as assets); *Data Valuation: Why It Matters & How It's Done*, ANMUT, https://www.anmut.co.uk/an-introduction-to-data-valuation/ (last visited Mar. 3, 2023) (emphasizing the importance of data valuation given the increased volume in recent times).

171. Jurcys, *supra* note 166.

172. *Id.*

173. *See* Emily Steel, Callum Locke, Emily Cadman & Ben Freese, *How Much Is Your Personal Data Worth?*, FIN. TIMES (June 12, 2013), https://ig.ft.com/how-much-is-your-personal-data-worth/.

174. Jurcys, *supra* note 166.

175. *See* S. Dixon, *Number of Monthly Active Facebook Users Worldwide as of 4th Quarter 2022*, STATISTA (Feb. 13, 2023), https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

asset to generate about $110 in advertising revenue per American user in 2018.[176] By another estimate, Meta, Facebook's parent company, may also earn as much as $900 annually per user by selling data to other companies.[177]

Algorithms for analyzing personal data use a combination of information from different sources.[178] In addition to web browsing and social media posts, data may be taken from the contents of emails and texts, credit card purchases, and almost anything else an individual does online that involves the input of personal information.[179] When combined with basic demographic information, algorithms can determine the interests, likes and dislikes, family background, political leanings, and sexual orientation of individuals.[180]

With the addition of genomic data that reveal the physiological makeup of individuals and brain data that can reveal their innermost thoughts, the potential for algorithms to determine every detail of an individual's behavior is vast.[181] The incentive to collect as much of that information as possible is obvious.[182] That incentive cries out for countervailing

176. Shapiro, *supra* note 168.

177. Jim Martin, *This Is How Much Money Facebook Earns from Your Data Each Year*, TECH ADVISOR (Jan. 28, 2022, 1:30 AM), https://www.techadvisor.com/article/745709/this-is-how-much-money-facebook-earns-from-your-data-each-year.html.

178. Shapiro, *supra* note 168.

179. *Id.*

180. *Id.*

181. *See* Stephen Rainey, Stéphanie Martin, Andy Christen, Pierre Mégevand & Eric Fourneret, *Brain Recording, Mind-Reading, and Neurotechnology: Ethical Issues from Consumer Devices to Brain-Based Speech Decoding*, 26 SCI. & ENG'G ETHICS 2295, 2297–98 (2020); James P. Evans & Michael S. Watson, *Genetic Testing and FDA Regulation: Overregulation Threatens the Emergence of Genomic Medicine*, 313 J. AM. MED. ASS'N 669, 669 (2015); *see also 29 Neurotech Companies Interfacing with Your Brain*, NANALYZE (Oct. 10, 2017), https://www.nanalyze.com/2017/10/29-neurotech-companies-interfacing-brain/ (giving examples of neurotech companies capitalizing from brain data); *Are Your Thoughts Your Own: "Neuroprivacy" and the Legal Implications of Brain Imaging*, REC. ASS'N BAR CITY N.Y., 2005, at 407, https://www2.nycbar.org/Publications/record/vol.%2060%20no.%202.pdf (discussing the privacy and legal implications of brain imaging and other neurodiagnostic techniques).

182. *See* Christopher Kuner, Fred H. Cate, Christopher Millard & Dan Jerker B. Svantesson, *Privacy—An Elusive Concept*, 1 INT'L DATA PRIV. L. 141, 141–42 (2011).

safeguards against abuses of their stewardship of such a sensitive asset.[183]

Legal precedents in the United States have favored those collecting personal data over the subjects of the data they collect. In the first case to address the issue, *Moore v. Regents of the University of California*, the California Supreme Court rejected a cancer patient's claim to a share of six billion dollars in proceeds from a cell line that a physician isolated from his spleen after removing it and patenting it.[184] In *Greenberg v. Miami Children's Hospital*, a federal district court ruled that individuals have no ownership interest in tissue samples taken by researchers and that they have no claim to royalties from a genetic test that was developed from those samples.[185] In *Washington University v. Catalona*, the United States Court of Appeals for the Eighth Circuit found that the University had the right to retain blood and tissue samples collected as part of genetic cancer research.[186] The research was conducted in the University's facilities in the face of a request from the researcher and his patients to transfer them to another university he had joined.[187]

C. *Expectations of Privacy*

While the range of possible intrusions into privacy have grown dramatically over the past several decades, public expectations have evolved as well. Surrendering private

183. Privacy takes on greater significance as individuals leave a growing assortment of traces of themselves by participating in online activities, which are increasingly difficult to avoid. Buttarelli, *supra* note 142 at 327. The central importance of privacy "is being questioned in an age where humans are submitting large quantities of traces of themselves, increasingly unwittingly, and as a by-product or condition of their participation in digital life." *Id.* at 325.

184. Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 480–82, 493, 497 (Cal. 1990) (en banc). While rejecting the patient's claim to a share of the proceeds, the Court did declare that he had the right to be informed of the physician's interest in the spleen removal procedure and to consent to it in advance. *Id.* at 484–86, 491–93.

185. 264 F. Supp. 2d 1064, 1074–76 (S.D. Fla. 2003). The plaintiffs were parents of children who were treated at Miami Children's Hospital for a rare genetic condition known as Canavan disease. *Id.* at 1066. The defendants were the researcher and the Hospital. *Id.*

186. Wash. Univ. v. Catalona, 437 F. Supp. 2d 985, 988, 1002–03 (E.D. Mo. 2006).

187. *Id.* at 1002–03.

information is the price for accessing a range of technologically complex services that add tremendous convenience to daily life, from searching the web, communicating with others around the globe and finding directions to a destination.[188] This is not to mention the convenience of paying for goods and services with a plastic card instead of cash or the monetary reward of obtaining discounts at retailers by using a loyalty card.[189] With conveniences such as these, much of the public seems to accept privacy intrusions as a necessary part of life despite the possibilities for abuse.[190] The expectations that Warren and Brandeis described no longer seem to be the norm.[191]

Nevertheless, awareness of threats to privacy is evident around the globe. In a worldwide survey, 78.5% of respondents agreed that privacy is a human right.[192] A clear majority supported this proposition across all regions, religions, ages, and genders.[193] However, there appear to be generational differences, at least in the United States.[194] While people of all ages are aware of cybersecurity risks, one study found that those born after 1997 are the least concerned.[195] On the other

188. *See* Buttarelli, *supra* note 142, at 327; *see also* Nica Latto, *A Day in Your Digital Life… and the Trail You Leave*, AVG SIGNAL BLOG, https://www.avg.com/en/signal/digital-day-in-the-life (Aug. 17, 2022) (detailing the average daily digital footprint of an individual).

189. *See* Vilius Petkauskas, *Loyalty for Data: What do Retailers Know About You?*, CYBER NEWS, https://cybernews.com/privacy/loyalty-for-data-what-do-retailers-know-about-you/ (Sept. 28, 2021); Helm, *supra* note 4.

190. BROOKE AUXIER, LEE RAINIE, MONICA ANDERSON, ANDREW PERRIN, MADHU KUMAR & ERICA TURNER, PEW RSCH. CTR., AMERICANS AND PRIVACY: CONCERNED, CONFUSED AND FEELING LACK OF CONTROL OVER THEIR PERSONAL INFORMATION 2 (2019).

191. *See* Warren & Brandeis, *supra* note 129, at 195.

192. HUANG & BASHIR, *supra* note 126, at 80.

193. *See id.* at 80–81.

194. *See* Mª Victoria Bordonaba-Juste, Laura Lucia-Palacios & Raúl Pérez-López, *Generational Differences in Valuing Usefulness, Privacy and Security Negative Experiences for Paying for Cloud Services*, 18 INFO. SYS. & E-BUSINESS MGMT. 35, 52–53 (2020). Older and younger generations differ in their willingness to pay for a variety of web-based services, including privacy and security features. *See id.* Moreover, "previous negative experience[s] related to privacy or security" had a different impact on willingness to pay for these services based on age group. *Id.* at 54.

195. *See* Adam Weir, *The Generational Gap in Cybersecurity and Privacy*, VONAGE, https://www.vonage.com/resources/articles/generational-gap-cybersecurity-privacy/ (last visited Mar. 3, 2023).

hand, another study found that three-quarters of respondents born between 1981 and 1996 are concerned about how social media companies use their data and, in particular, location information.[196]

These surveys explored general expectations of privacy.[197] They reflect attitudes concerning common online behavior that discloses information pertaining to personal attributes under the control of the individual and subject to change.[198] Sensitive biometric data present a different level of risk.[199] Genetic and brain data are not under the control of, or even known to, the individual who discloses them.[200] In fact, discovering the attributes genetic and brain data reveal is the reason people seek those kinds of tests to begin with.[201] Concerns over privacy may grow as the hazards of sharing that information become more widely known.

III. LEGAL PROTECTIONS AND THEIR SHORTCOMINGS

For purposes of understanding the relevant law, databases containing genomic and brain data can be divided into three categories. The first category is clinical databases that contain information on patients and are maintained by providers, such as health systems, to aid in patient care.[202] The second category

196. *Concerns About Online Data Privacy Span Generations*, INTERNET INNOVATION ALL. (July 25, 2019), https://internetinnovation.org/general/concerns-about-online-data-privacy-span-generations/.

197. *See, e.g.*, Huang & Bashir, *supra* note 125, at 80 (finding that "[78.5%] of participants agreed that privacy is a human right" and thus "a right to be let alone"); *supra* notes 192–96 and accompanying text.

198. *See supra* notes 192–96 and accompanying text; INTERNET INNOVATION ALL., CONSUMER DATA PRIVACY CONCERNS 5, 9, 13 (2019) (surveying attributes like "personal financial information," "online searches," and "location information").

199. *See Genetic Information Privacy*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/genetic-information-privacy (last visited Mar. 3, 2023) (explaining that "[a]s accessing and recording genetic information progresses, it raises some serious issues" in areas like employment, newborn screening, and law enforcement).

200. *See* discussion *supra* Section I.C.

201. *See* discussion *supra* Sections I.A–.B.

202. *See, e.g.*, Patricia Robin McCartney, *Clinical Databases: Electronic Health Records and Repositories*, 38 AM. J. MATERNAL/CHILD NURSING 186, 186 (2013) (describing the way hospital systems use patient information to provide the best medical care).

is research databases that are maintained by universities and other research organizations as tools for biomedical research.[203] The third category is DTC databases that are maintained by for-profit companies to provide analyses to customers who submit data samples.[204] The legal status of the data they collect is discussed in Part IV.[205]

A. *Federal Laws Protecting Clinical Data*

Data collected as part of a patient's diagnosis and treatment are shielded from unauthorized disclosure by the Health Insurance Portability and Accountability Act (HIPAA)[206] and regulations known as the Privacy Rule issued by the federal Department of Health and Human Services (DHHS) under it.[207] Under the Privacy Rule, patient information, known as "Protected Health Information" (PHI), may not be disclosed without a patient's consent, and DHHS can impose penalties for violations.[208] Genetic data collected as part of a patient's care fall under the definition of PHI.[209] This prohibits disclosure to marketers and data aggregators.[210]

However, the law has numerous limits and exceptions. The Privacy Rule only applies to data collectors known as "Covered Entities," a category that includes providers, payers, and insurance data clearinghouses.[211] It does not apply to other persons or entities who may be in possession of PHI.[212] The data

203. *See, e.g.*, *Human Brain Transcriptome*, HBATLAS, https://hbatlas.org/ (last visited Feb. 7, 2023).

204. *See, e.g.*, *AncestryDNA – Frequently Asked Questions*, ANC., https://www.ancestry.com/dna/en/legal/us/faq (last visited Mar. 3, 2023) (describing Ancestry's database as "one of the most comprehensive and unique collections of DNA samples from people around the world").

205. *See* discussion *infra* Part IV.

206. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

207. 45 C.F.R. §§ 160.101–552, 164.102–106, 164.500–534. (2023).

208. *Id.* §§ 164.502(a), 160.402(a).

209. *See id.* § 164.502(a)(5)(i).

210. *See id.* § 164.508(a)(1), (3)–(4).

211. *Id.* §§ 160.102(a), 103.

212. *See id.* § 160.102(a)–(b).

may be disclosed without consent to other clinicians involved in a patient's care, to insurers and employers that pay for care, and within a hospital or health system for administrative operations.[213] The data must also be disclosed to public health authorities upon request, in response to a court order, and to business partners who agree to honor Privacy Rule protections.[214] Additionally, the data may be shared with researchers, if measures are taken to deidentify them,[215] by deleting personally identifying information such as names, birth dates, and home addresses.[216] Genomic data are considered deidentified if the prescribed elements are deleted,[217] however as described in Part I, researchers are increasingly able to reidentify patients by combining genomes with publicly available information.[218]

B. *Federal Laws Protecting Research Data*

Subjects of biomedical research are protected by the Common Rule, a regulation issued jointly by the U.S. Department of Health and Human Services and fifteen federal agencies concerning research that they fund.[219] Authority to issue the rule stems from the National Research Act of 1974.[220] The core protection is that any federally funded research that involves human subjects be reviewed by an Institutional Review Board (IRB), a committee housed at the institution that conducts the

213. *Id.* §§ 164.506(a), 164.512(b)(1)(v), (d)(1).

214. *Id.* §§ 164.512(b)(1)(i), (e)(1), 164.502(e).

215. *Id.* § 164.512(i)(1).

216. *Id.* § 164.514(a)–(b).

217. *See* OFF. FOR C.R., GUIDANCE REGARDING METHODS FOR DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION IN ACCORDANCE WITH THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) PRIVACY RULE 6–8 (2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf; 45 C.F.R. § 164.514(b)(2).

218. *See supra* Section I.A.

219. *See* 45 C.F.R. § 46.101; Jerry Menikoff, Julie Kaneshiro & Ivor Pritchard, *Revised Common Rule*, U.S. DEPT. OF HEALTH & HUM. SERVS., https://www.hhs.gov/ohrp/regulations-and-policy/regulations/finalized-revisions-common-rule/index.html (Jan. 19, 2017).

220. National Research Act, Pub. L. No. 93-348, 88 Stat. 342 (1974) (codified as amended at 42 U.S.C. Ch. 6A).

research.[221] IRBs are charged with minimizing risks to subjects and weighing them in relation to the expected benefits of the research.[222] An important aspect of this role is to ensure that subjects provide informed and voluntary consent to these risks, including threats to their privacy.[223] A similar set of regulations requires IRB review for clinical research that supports an application for approval of a new drug by the federal Food and Drug Administration (FDA).[224]

The application of the Common Rule is limited in that it only applies to research funded by one of the fifteen federal agencies that issued it, or if the research is conducted as part of testing a new drug.[225] It does not apply to privately funded or self-funded studies.[226] Many research organizations apply IRB review to all research, regardless of funding source, however, they are not legally required to do so.[227]

Moreover, revisions to the Common Rule issued in 2018 permitted researchers greater leeway in collecting and using data on subjects.[228] Under the revisions, consent is no longer needed for sharing data that are deidentified and subjects can be asked for "broad consent," which permits data to be used in

221. 42 U.S.C. § 289(a).

222. *IRBs: ORI Introduction to RCR: Chapter 3. The Protection of Human Subjects*, U.S. DEPT. OF HEALTH & HUM. SERVS.: OFF. OF RSCH. INTEGRITY, https://ori.hhs.gov/content/chapter-3-The-Protection-of-Human-Subjects-IRBs (last visited Mar. 3, 2023).

223. *Id.*

224. 21 C.F.R. § 56.103 (2023).

225. *Id.*; 45 C.F.R. § 46.101.

226. *Is All Human Research Regulated?*, U.S. DEPT. OF HEALTH & HUM. SERVS.: OFF. FOR HUM. RSCH. PROTS., https://www.hhs.gov/ohrp/education-and-outreach/about-research-participation/protecting-research-volunteers/other-research/index.html (Jan. 28, 2022).

227. *See, e.g.*, *FAQs*, DEPAUL OFF. OF RSCH. SERVS., https://offices.depaul.edu/research-services/research-protections/irb/Pages/faq.aspx (last visited Apr. 9, 2023) (explaining how all University research that involves human subjects requires IRB review, regardless of the funding source); *see also Is All Human Research Regulated?*, *supra* note 226.

228. *See* 45 C.F.R. § 46.101(l); *see also* Stephen J. Rosenfeld, *Informed Consent and the Revised Common Rule*, HARV. MED. SCH. CTR. FOR BIOETHICS (June 1, 2019), https://bioethics.hms.harvard.edu/journal/consent-common-rule (explaining how the goal of the revised Common Rule is to "increase participant participation while removing unnecessary burdens on the conduct of research that do not serve such protection").

subsequent studies without additional consent.[229] Genomic and brain data may thereby be shared by the researcher who collected them if individual identities are not attached, although assuring continuing anonymity is becoming nearly impossible.[230]

C. *Other Laws Protecting Privacy*

Companies that collect data within the European Union (EU) or on EU citizens are subject to the General Data Protection Regulation (GDPR).[231] That law requires entities that collect and maintain data online, including biometric data, to provide data subjects with various rights.[232] These include the right to access their own data, to correct errors, to restrict transfer, and to have data deleted.[233] The law designates "special categories of personal data" that receive extra protection, including genetic data, biometric data used for identification, and health data.[234] Data within this category are considered especially sensitive because they relate to deeply personal attributes and to such basic rights as freedom of thought.[235] Brain data would clearly also fall into this category.[236]

Penalties for violations can be substantial—up to twenty million euros (equivalent to roughly twenty-one million U.S.

229. 45 C.F.R. § 46.104(d)(2)(i), (d)(7), (d)(8), 46.116(d).

230. *See* 45 C.F.R. § 46.104(d)(2)(i); *supra* notes 48–52 and accompanying text.

231. Council Regulation 2016/679, art. 3, 2016 O.J. (L 119) 32, 33 (EU).

232. *See Biometric Data and Privacy Laws (GDPR, CCPA/CPRA)*, *supra* note 21; *Rights of Data Subjects Under GDPR*, HIPAA J. (June 11, 2021), https://www.hipaajournal.com/rights-of-data-subjects-under-gdpr/.

233. *Rights of Data Subjects Under GDPR*, *supra* note 232.

234. *What Is Special Category Data?*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/ (last visited Apr. 14, 2023) (internal quotation marks omitted). Other kinds of data within the "special categories of personal data" include "data revealing racial or ethnic origin," political opinions, "religious or philosophical beliefs," trade union membership, sex life, and sexual orientation. *Id.*

235. *See id.* Other personal freedoms that may be jeopardized by "special categories of personal data" include conscience, religion, expression, "assembly and association," bodily integrity, "private and family life," and nondiscrimination. *Id.*

236. *See id.*

dollars), or 4% of the prior year's revenues, whichever is greater.[237] However, for an individual to seek remedies under the law, they must know that their information is being maintained and by whom.[238] For a relative of a genetic testing subject or an acquaintance identified from brain data, knowing their information is being maintained and by whom is almost impossible.[239]

The State of California has enacted its own privacy law modelled on the GDPR.[240] The California Consumer Privacy Act (CCPA) permits individuals whose information is maintained in online databases to access their information, make corrections, and request deletion.[241] However, CCPA applies only to the for-profit holders of data and to data collected during the previous twelve months.[242] Its penalties are also much milder than those contained in the GDPR, and it allows a private right of action only for breaches of personal information.[243]

In addition to California, four other states have enacted data privacy laws of their own.[244] These include Colorado, Connecticut, Utah, and Virginia.[245] These laws vary in scope, however they apply only residents for the states that enacted

237. Ben Wolford, *What Are the GDPR Fines?*, GDPR, https://gdpr.eu/fines/ (last visited Apr. 10, 2023); *see* Council Regulation 2016/679, *supra* note 231, at 83; *see also* 20,000,000 EUR to USD – Convert Euros to US Dollars, XE CURRENCY CONVERTER, https://www.xe.com/currencyconverter/convert/?Amount=20000000&From=EUR&To=USD (last visited Apr. 14, 2023).

238. *See* Council Regulation 2016/679, *supra* note 231, at 80.

239. *See What Should We Do If the Request Involves Information About Other Individuals?*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/right-of-access/information-about-other-individuals/ (last visited Apr. 14,, 2023).

240. *See Biometric Data and Privacy Laws (GDPR, CCPA/CPRA)*, *supra* note 21.

241. California Consumer Privacy Act, CAL. CIV. CODE §§ 1798.105, 1798.110 (Deering 2022).

242. *See id.* §§ 1798.130(a)(3)–(5), 1798.140(c).

243. *See id.* §§ 1798.140(v), 1798.150; *see also* Council Regulation 2016/679, *supra* note 231, at 8.

244. Sheila A. Millar & Tracy P. Marshall, *The State of U.S. State Privacy Laws: A Comparison*, NAT'L L. REV. (May 24, 2022), https://www.natlawreview.com/article/state-us-state-privacy-laws-comparison.

245. *Id.*

them.[246] Moreover, none of these laws fully allow a private right of action,[247] and the patchwork of state laws can make it difficult for data subjects to determine what protections apply to them.[248]

D. *Laws Restricting the Use of Data*

If sensitive data are nonetheless disclosed through a gap in the laws or through deliberate noncompliance, there are still legal protections against using them for discrimination. The Genetic Information Nondiscrimination Act prohibits the use of genetic data in certain spheres of business activity, including health insurance and employment.[249] However, it does not apply to disability, life, and long-term care insurance,[250] and the protection for health insurance was made irrelevant by the Affordable Care Act, which prohibits the use of any medical information in the offer and pricing of individual health insurance policies.[251] The law's protections also do not apply to education, housing, and mortgage lending.[252]

The Americans with Disabilities Act prohibits discrimination in employment and in access to public services based on a disability.[253] Individuals may not be denied employment or promotion or access to services such as hotel accommodations, restaurants, entertainment, education, and medical care based

246. *See id.*; *see also A Comprehensive Guide to the US State Privacy Laws*, DATAGRAIL (Oct. 11, 2022), https://www.datagrail.io/blog/data-privacy/us-states-with-data-privacy-laws/.

247. *See* Millar & Marshall, *supra* note 244. A new law enacted in the state of Washington, the My Health, My Data Act, adds a private right of action and covers a broad range of medical, biometric, and personal information. H.R. 1155, 68th Leg., Reg. Sess. (Wa. 2023); *see* Cat Zakrzewski, *Washington Becomes First State to Adopt Health Data Protections Post-Roe*, WASH. POST, https://www.washingtonpost.com/technology/2023/04/27/washington-reproductive-health-law/ (April 27, 2023, 6:53 PM).

248. *See generally id.* (explaining the varying protections afforded to residents of the five states with enacted data privacy laws).

249. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881.

250. *Genetic Discrimination*, NAT'L. HUM. GENOME RSCH. INST., https://www.genome.gov/about-genomics/policy-issues/Genetic-Discrimination (Jan. 6, 2022).

251. *See* Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010).

252. *See Genetic Discrimination*, *supra* note 250.

253. Americans with Disabilities Act of 1990, Pub. L. No. 101-336, 104 Stat. 327.

on a condition that limits one or more essential life activities, a history of having had such a condition, or the perception that an individual has one.[254] The law is administered and enforced by the federal Equal Employment Opportunity Commission (EEOC).[255] Agency regulations interpret the scope of such conditions as excluding genetic susceptibilities that have not yet been manifested as a disease.[256] Therefore, the law would provide no protection to a database subject whose information reveals a genetic trait that has not yet caused a disabling condition.[257] For brain data, protection would similarly only be available for data subjects whose EEG readings indicate a neurological trait that is not pathological.[258]

If genetic traits correspond with a particular race or ethnicity, Title VI of the Civil Rights Act of 1964[259] may apply. That law prohibits discrimination in employment, housing, and public accommodations based on race, color, or nation origin.[260] However, the burden of proof for bringing such a claim would be substantial.[261] A data subject would have to establish that the genetic information that formed the basis for discrimination corresponded with a racial or ethnic category.[262]

E. *Other Legal Oversight*

In addition to laws concerning data privacy and use, the services of genomic and neurotechnology testing companies are

254. *See* 28 C.F.R. §§ 36.102, 36.104–.105 (2016); *Questions and Answers on the Final Rule Implementing the ADA Amendments Act of 2008*, U.S. EQUAL EMP. OPPORTUNITY COMM'N (Mar. 25, 2011), https://www.eeoc.gov/laws/guidance/questions-and-answers-final-rule-implementing-ada-amendments-act-2008.

255. *See What You Should Know About the EEOC and Enforcement of the Americans with Disabilities Act*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/wysk/what-you-should-know-about-eeoc-and-enforcement-americans-disabilities-act (last visited Apr. 14, 2023); 42 U.S.C. §§ 12117, 12206(a), (c).

256. *See* 28 C.F.R. § 36.10.

257. *See id.*

258. 28 C.F.R. § 36.105.

259. *See* The Civil Rights Act of 1964, 42 U.S.C. §§ 1981–2000h-6.

260. *See id.* §§ 2000a, 2000e-2 to e-3, 2000d.

261. *See id.* § 2000e-2(k).

262. *Id.* § 2000e-2(k)(1)(A)(i).

regulated for safety and effectiveness by the federal Food and Drug Administration (FDA) and for truthfulness in advertising by the Federal Trade Commission (FTC).[263] The FDA must approve a new drug or medical device before it may be marketed, and to receive approval, a manufacturer must present evidence that the drug or device is safe and effective.[264] However, to fall under this requirement, a drug or device must be promoted for a medical use to diagnose, treat, or cure a disease or condition.[265] Tests that are merely claimed to satisfy a customer's curiosity, for example about their ancestry or psychological state, or to enhance their overall "wellness," are exempt.[266] Moreover, there is no requirement or even industry custom for experts to help customers interpret the results.[267]

There are some applications of genetic and neurotechnology tests that serve medical purposes, and FDA approval is required to market them.[268] The agency must also approve any

263. *See What Does FDA Regulate?*, FOOD & DRUG ADMIN (Jan. 18, 2022), https://www.fda.gov/about-fda/fda-basics/what-does-fda-regulate; s*ee also GeneLink Settles with FTC over DNA Product Claims*, TRUTH IN ADVERT. (May 12, 2014), https://truthinadvertising.org/articles/genelink-settles-ftc-dna-product-claims/.

264. *Is It Really 'FDA Approved?'*, FOOD & DRUG ADMIN. (May 10, 2022), https://www.fda.gov/consumers/consumer-updates/it-really-fda-approved.

265. *See also Classification of Products as Drugs and Devices and Additional Product Classification Issues*, FOOD & DRUG ADMIN., https://www.fda.gov/regulatory-information/search-fda-guidance-documents/classification-products-drugs-and-devices-and-additional-product-classification-issues (July 12, 2018); Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 321(g)–(h) (2010).

266. *Direct-to-Consumer Tests*, FOOD & DRUG ADMIN (Dec. 20, 2019), https://www.fda.gov/medical-devices/in-vitro-diagnostics/direct-consumer-tests; FOOD & DRUG ADMIN, GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES 3 (2019), https://www.fda.gov/media/90652/download.

267. *See generally* Amie C. O'Donoghue, Helen W. Sullivan, Pamela A. Williams, Claudia Squire, Kevin R. Betts, Jessica Fitts Willoughby & Sarah Parvanta, *Consumers' Understanding of FDA Approval Requirements and Composite Scores in Direct-to-Consumer Prescription Drug Print Ads*, 21 J. HEALTH COMMC'N 927 (2016); *see also Is It Really 'FDA' Approved'?*, *supra* note 264 (demonstrating examples of how the FDA does not require nor is it industry custom for experts to assist customers interpret results).

268. Laboratories that perform testing for clinical purposes are regulated for quality by the Centers for Disease Control and Prevention in conjunction with the Centers for Medicare & Medicaid Services and the FDA under the Clinical Laboratory Improvement Act of 1988. *See About CLIA*, CTRS. FOR DISEASE CONTROL & PREVENTION, (Aug. 6, 2018), https://www.cdc.gov/clia/about.html; 42 U.S.C. § 263a; 42 C.F.R. § 493.1–.2001. The FDA regulates the equipment used in the tests as medical devices under the Food and Drug Administration Safety and Innovation

marketing materials that include claims about medical benefits.[269] The DTC company 23andMe has received FDA approval for genetic tests for detecting ten diseases.[270] Neurotechnology tests that diagnose and treat emotional disorders—such as depression and anxiety—and neurological conditions—such as Parkinson's disease, Alzheimer's disease, and epilepsy—must also go through the FDA approval process as medical devices.[271] The same requirement applies to invasive tests that implant sensors.[272]

Customers who use medical applications of these technologies are, therefore, protected, at least to some extent, from products that are unsafe or ineffective. However, customers who purchase tests for other purposes have no assurance that an external body has assessed their value.[273] The FDA also does not oversee the use of DTC customer test data,

Act of 2012. *See, e.g.*, Bethany La Couture, *Primer: FDA and Regulation of Laboratory Developed Tests*, AM. ACTION F. (Nov. 17, 2015), https://www.americanactionforum.org/insight/primer-fda-and-regulation-of-laboratory-developed-tests/; Food and Drug Administration Safety and Innovation Act, Pub. L. No. 112-144, § 1143, 126 Stat. 993 (2012) (setting forth a sunset provision whereby the FDA could not regulate "laboratory-developed tests" without congressional notification).

269. *See, e.g.*, *FDA Allows Marketing of First Direct-to-Consumer Tests That Provide Genetic Risk Information for Certain Conditions*, FOOD & DRUG ADMIN., https://www.fda.gov/news-events/press-announcements/fda-allows-marketing-first-direct-consumer-tests-provide-genetic-risk-information-certain-conditions (Mar. 28, 2018); *see generally* 21 C.F.R. § 814.1–.126 (setting forth premarket approval of medical devices).

270. *See* Abigail Abrams, *The FDA Just Approved At-Home DNA Tests for 10 Diseases*, TIME (Apr. 6, 2017, 3:48 PM), https://time.com/4729600/fda-approval-23andme-dna-tests/.

271. *See, e.g.*, Food Drug and Cosmetic Act, 21 U.S.C. § 321(h)(1); 21 C.F.R. §§ 800–898, 900, 900.1–900.25, 1000–1050, 1100–1150, 1210–1299; *Code of Federal Regulations (CFR)*, U.S. FOOD & DRUG ADMIN. (Mar. 22, 2018), https://www.fda.gov/medical-devices/overview-device-regulation/code-federal-regulations-cfr.

272. *See, e.g.*, *FDA Approves First Continuous Glucose Monitoring System with a Fully Implantable Glucose Sensor and Compatible Mobile App for Adults with Diabetes*, FOOD & DRUG ADMIN. (June 25, 2018), https://www.fda.gov/news-events/press-announcements/fda-approves-first-continuous-glucose-monitoring-system-fully-implantable-glucose-sensor-and; *see, e.g.*, 21 U.S.C. § 321(h)(1); 21 C.F.R. §§ 800–98, 900, 900.1–.25, 1000–50, 1100–50, 1210–99; *Code of Federal Regulations (CFR)*, *supra* note 271.

273. *See Direct-to-Consumers Test*, FOOD & DRUG ADMIN. (Dec. 20, 2019), https://www.fda.gov/medical-devices/in-vitro-diagnostics/direct-consumer-tests.

whether in the form of genomics or neurotechnology results, for nonmedical purposes.[274]

Nevertheless, there is regulatory protection for customers of nonmedical tests against false advertising. Although the FTC does not assess safety and effectiveness, it does enforce prohibitions against claims in these regards that are not true.[275] It has taken numerous actions against companies making health claims, for example against sellers that claimed their product protected against the Zika virus.[276] In 2006, the FTC published a fact sheet warning consumers about the limits of at-home genetic tests.[277]

The agency has also taken actions against neurotechnology companies for false claims. For example, in 2016, it sued a company known as Lumosity for claiming that its brain-training games could enhance concentration and could decrease cognitive impairment in patients with Alzheimer's disease.[278] In 2016, it reached a settlement in a suit against a company known as Carrot Neurotechnology that claimed its

274. *See, e.g.*, *id.*

275. *Enforcement Policy Statement on Food Advertising*, FED. TRADE COMM'N (May 13, 1994), https://www.ftc.gov/legal-library/browse/enforcement-policy-statement-food-advertising; *see also* 21 C.F.R. § 202.1 (e)(5)(ii) (requiring truthfulness in drug advertising by the FDA); 21 U.S.C. § 601(n)(1) (authorizing the USDA by prohibiting the labeling of meat or products that are "false or misleading in any particular"); 21 U.S.C. § 453(h)(1) (same, but for poultry products).

276. *See FTC Sends Warning Letters to Online Sellers Making Zika Virus-Protection Claims*, FED. TRADE COMM'N (Aug. 5, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/08/ftc-sends-warning-letters-online-sellers-making-zika-virus-protection-claims; *see also Commercial Weight Loss Products and Programs What Consumers Stand to Gain and Lose*, FED. TRADE COMM'N (Mar. 1998), https://www.ftc.gov/reports/commercial-weight-loss-products-programs-what-consumers-stand-gain-lose (detailing the FTC enforcement actions brought against companies making unsubstantiated health claims through weight loss clinics).

277. *See* FED. TRADE COMM'N, FTC FACTS FOR CONSUMERS, AT-HOME GENETIC TESTS: A HEALTHY DOSE OF SKEPTICISM MAY BE THE BEST PRESCRIPTION 3 (2006), https://permanent.fdlp.gov/lps103454/hea02.pdf.

278. *See* Fed. Trade Comm'n v. Lumos Labs, Inc., No. 3:16-cv-00001, at *1, *5–6 (N. D. Cal. Jan. 8, 2016); Mike Brunker, *Lumosity to Pay $2M to Settle FTC Charges Over 'Brain Training' Ads*, NBC NEWS, https://www.nbcnews.com/business/consumer/lumosity-pay-2m-settle-ftc-charges-over-brain-training-ads-n490571 (Jan. 5, 2016, 12:14 PM); *Lumosity to Pay $2 Million to Settle FTC Deceptive Advertising Charges for Its "Brain Training" Program*, FED. TRADE COMM'N (Jan. 5, 2016), https://www.ftc.gov/news-events/news/press-releases/2016/01/lumosity-pay-2-million-settle-ftc-deceptive-advertising-charges-its-brain-training-program.

technology could improve vision.[279] The FTC has also expressed interest in taking steps to safeguard data privacy,[280] although they have been limited to date. As far back as 1995, the agency initiated a privacy initiative, although it has engendered little regulatory activity.[281] However, it recently announced a new data privacy initiative that might inject new vigor into its efforts.[282] The agency is well-positioned to take on the issue under its authority to protect consumers against "unfair and deceptive [trade] practices."[283] It could be the mechanism for closing some of the gaps left by federal and state laws, although aggressive enforcement would require additional resources and expertise.

IV. THE SPECIAL CIRCUMSTANCES OF DIRECT-TO-CONSUMER DATA

The largest databases are those of DTC testing companies,[284] which collect genetic data from and maintain information on more than twenty-five million people.[285] Those that collect brain data are, for the most part, newer, but they include dozens of

279. *See In re* Carrot Neurotechnology, Inc., No. 142 3132, at *4–5, *10 (2016).

280. *See* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2018, at 2 (2018), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.

281. *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 2 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf ("In April 1995, staff held its first public workshop on privacy on the Internet, and in November of that year the Commission held hearings on online privacy . . . .").

282. *See* Joseph Duball, *FTC Officially Launches Privacy Rulemaking Endeavor*, IAPP (Aug. 11, 2022), https://iapp.org/news/a/ftc-officially-launches-privacy-rulemaking-endeavor/.

283. *See* Federal Trade Commission Act, 15 U.S.C. §§ 45(a)(4), (B).

284. Margaret O'Brien, *Who Has the Largest DNA Database? (2023)*, DATA MINING DNA (July 17, 2021), https://www.dataminingdna.com/who-has-the-largest-dna-database/ (suggesting that the five largest commercial genomic databases have data on almost forty million people).

285. *See* Juliana Szucs, *23andMe and Ancestry.com Partner to Extend Access to Genetic Ancestry Expertise*, 24-7 FAM. HIST. CIRCLE (Sept. 9, 2008), https://blogs.ancestry.com/circle/?p=2865; Eric Rosenbaum, *5 Biggest Risks of Sharing Your DNA with Consumer Genetic-Testing Companies*, CNBC, https://www.cnbc.com/2018/06/16/5-biggest-risks-of-sharing-dna-with-consumer-genetic-testing-companies.html (June 16, 2018, 2:18 PM); Brishette Mendoza & Amadou Diallo, *The Best DNA Testing Kit*, N.Y. TIMES: WIRECUTTER, https://www.nytimes.com/wirecutter/reviews/best-dna-test/ (Dec. 1, 2022).

start-ups that are attracting significant investment funding.[286] Yet, genetic data collected by these companies are subject to the fewest legal protections.[287]

A. *Gaps in Federal Laws*

Neither of the federal laws described in section III that apply to clinical and research data apply to data collected by DTC testing companies.[288] Even though some of the information DTC companies collect would qualify as PHI under HIPAA, the companies are not considered Covered Entities subject to its provisions.[289] Although some DTC companies conduct research on the data of individuals who contribute samples and are therefore human subjects, little of this research is funded by federal agencies.[290] While data are often shared with pharmaceutical companies for drug development, the data are not collected as part of clinical trials that form part of applications for approval of new drugs.[291] Moreover, there are no federal laws that prohibit DTC companies from sharing genetic data, or brain data, with third parties.[292]

286. *See 21 Neurotech Startups to Watch: Brain-Machine Interfactes, Implantables, and Neuroprosthetics*, CBINSIGHTS (Jan. 28, 2019), https://www.cbinsights.com/research/neurotech-startups-to-watch/.

287. *Privacy in Genomics*, *supra* note 95.

288. *See id.*; *see also* discussion *supra* Part III.

289. *See Health Privacy: HIPAA Basics*, PRIV. RTS. CLEARINGHOUSE, https://privacyrights.org/consumer-guides/health-privacy-hipaa-basics (Feb. 1, 2015).

290. *See* Sarah Schmidt, *9 Leading Companies in Direct-to-Consumer Genetic Testing*, MKT. RSCH.COM (Apr. 6, 2016), https://blog.marketresearch.com/9-leading-companies-in-direct-to-consumer-genetic-testing; *see also Definition of Human Subjects Research*, NAT'L INST. OF HEALTH: GRANTS & FUNDING, https://grants.nih.gov/policy/humansubjects/research.htm (Jan. 13, 2020); INST. OF MED. COMM. ON ASSESSING GENETIC RISKS, ASSESSING GENETIC RISKS: IMPLICATIONS FOR HEALTH AND SOCIAL POLICY 243 (Lori B. Andrews, Jane E. Fullarton, Neil A. Holtzman & Arno G. Motulsky eds., 1994) ("Medicaid reimbursement is available for *some* genetic laboratory testing services, but . . . estimates indicate that Medicaid pays less than half of the actual charges for some of the genetic tests for which it reimburses.") (emphasis added).

291. *See* Schmidt, *supra* note 290; *A Genetic Data Matchmaking Service for Researchers*, ILLUMINA, https://www.illumina.com/science/customer-stories/icommunity-customer-interviews-case-studies/short-sano-genetics.html (last visited Apr. 14, 2023) (remarking that "there [are] several ways that DTC genetic testing could be improved," such as by "allow[ing] . . . access [to data] as part of . . . clinical trials").

292. *Privacy in Genomics*, *supra* note 95.

B. *Companies' Terms of Service*

The primary legal protection for customers of DTC testing companies are the companies' terms of service (TOS), which users are required to accept.[293] These usually include privacy policies.[294] Customers could pursue violations of TOS as breaches of contract, although the task of proving noncompliance could be daunting.[295]

Moreover, explicit privacy policies are often lacking in TOS, and when they are present, the policy is often vague and subject to change.[296] A review of privacy policies posted on the websites of ninety DTC genetic testing companies revealed the limits of their protection.[297] Among the more striking findings were that 39% of companies posted no privacy policy at all, 89% had only vague information about privacy, 45% stated that they kept data indefinitely, 95% had no information on company actions in the event of a data breach, and 33% had no contact information for making further inquiries.[298]

Of particular concern, almost every policy permitted the company to make changes to the TOS without prior notice to customers.[299] Such changes could be effectuated unilaterally by the company or by another entity that obtains its database through corporate acquisition.[300] In other words, even a

293. *See, e.g.*, *TOS Violations: Everything You Need to Know*, UPCOUNSEL, https://www.upcounsel.com/tos-violations (last visited Apr. 14, 2023); Michelle Fernandes Martines, Logan T. Murry, Liesl Telford & Frank Moriarty, *Direct-to-Consumer Genetic Testing: An Updated Systematic Review of Healthcare Professionals' Knowledge and Views, and Ethical and Legal Concerns*, 30 EURO. J. HUM. GENETICS 1331, 1341 (2022); *How Do I Choose a Direct-to-Consumer Genetic Testing Company?*, MEDLINE PLUS, https://medlineplus.gov/genetics/understanding/dtcgenetictesting/dtcchoosing/ (June 21, 2022).

294. *See* James W. Hazel & Christopher Slobogin, *Who Knows What, and When?: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies*, 28 CORNELL J.L. & PUB. POL.'Y 35, 48 (2018).

295. *TOS Violations: Everything You Need to Know*, *supra* note 293.

296. *See* Hazel & Slobogin, *supra* note 294, at 48, 65.

297. *See id.* at 48.

298. *Id.* at 48, 51, 53, 64.

299. *See id.* at 49.

300. *See id.* at 49, 56.

consumer-friendly policy is no guarantee of protection in the future.

The nature of these findings is reflected in a review of the privacy policies of two genetic testing and two neurotechnology companies posted on the companies' websites.[301] The policy of 23andMe, one of the largest DTC genetic testing companies, contains several provisions that are favorable to customers.[302] It permits them to access all personal information that the company maintains, to request deletion, and to receive the data in a form that can be transferred to another entity.[303] However, the Company reserves the right to modify the policy at any time.[304] While 23andMe promises to provide advance notice of any changes and to let customers cease using its services, it would be difficult for a customer to retrieve data that have already been shared with another entity.[305]

The policy of another major DTC genetic testing company, Ancestry, is considerably less protective.[306] It enables the company to collect data on the customer's interactions with it on social media and to share all of the information it has on customers with third parties for analysis for the purpose of targeted advertising.[307] The policy also permits the company to share customer information with an entity that acquires it either by purchase or merger or through bankruptcy.[308] In the event of

301. *See, e.g.*, *id.* at 38–39; *infra* notes 302–14.

302. *See Your Privacy Comes First*, 23ANDME, https://www.23andme.com/privacy/ (last visited Apr. 14, 2023).

303. *Id.*

304. *Terms of Service*, 23ANDME, https://www.23andme.com/legal/terms-of-service/ (June 8, 2022).

305. *See id.*; *see also Data Sharing*, 23ANDME, https://www.23andme.com/legal/privacy/#data-sharing (Dec. 14, 2022); *Research Participation and Consent*, 23ANDME, https://customercare.23andme.com/hc/en-us/articles/212195708-Research-Participation-and-Consent (last visited Apr. 14, 2023).

306. *See Your Privacy*, ANC. (Jan. 26, 2023), https://www.ancestry.com/c/legal/privacystatement.

307. *See id.*

308. *See id.*

an acquisition, the Privacy Policy will continue to apply, although the acquiring entity could change it at a later date.[309]

The privacy policies of two leading brain data companies are similarly lax. Emotiv reserves the right to collect personal data beyond that shared with it by customers when third parties, including business partners, provide it and when it is automatically collected in connection with a customer's use of its services.[310] It also explicitly reserves the right to change its policy at any time.[311] OpenBCI reserves the right to collect data from customers' social media accounts and from customer communications using social media.[312] The scope of data that can be collect is expanded even further by including any information a customer posts on social media while using the Company's services and "[a]ny other information which you voluntarily submit to us during the use of our Services."[313] As with the other Companies reviewed, OpenBCI reserves the right to change its policy at any time.[314]

V. PROPOSALS FOR REFORM

The most serious potential harms of unauthorized disclosure of genomic and brain data have yet to be realized. However, the threat is real. The danger is especially acute for data maintained by DTC testing companies, whose data practices are subject to minimal external oversight.[315] Those legal protections that exist are limited.[316] The need for reform is clear.

309. *See id.*; *Ancestry Terms and Conditions*, ANC., https://www.ancestry.com/c/legal/termsandconditions_2019_10_15 (Oct. 15, 2019).

310. *EMOTIV Privacy Policy*, EMOTIV, https://id.emotivcloud.com/eoidc/privacy/privacy_policy/ (Aug. 25, 2020).

311. *See id.*

312. *Privacy & Security*, OPENBCI DOCUMENTATION, https://docs.openbci.com/FAQ/Privacy/ (July 28, 2021).

313. *Id.*

314. *See id.*

315. *See* discussion *supra* Section IV.A.

316. *See supra* Parts III–IV.

Legislation has been proposed in Congress to protect privacy on a national basis.[317] The American Data Privacy Protection Act (ADPPA)[318] would set uniform standards for a broad range of data defined as "information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique identifiers."[319] Among other provisions, it would require "data minimization"; impose special requirements on the collection of geolocation and biometric information, "nonconsensual intimate images," and other sensitive data; require disclosure of the data companies collect, their uses, and length of retention; provide consumers with "the right to access, correct, and delete their data"; and prohibit the use of data in ways that discriminate.[320]

For "[l]arge [d]ata [h]olders," the legislation requires "an algorithm impact assessment" for "algorithms that may cause . . . harm to an individual."[321] It would prohibit targeted advertising to children, defined as anyone below the age of seventeen, without parental consent.[322] Enforcement authority would be housed in the FTC, and there would be a private right of action.[323] However, a particularly controversial provision

317. *See, e.g.*, Marguerite Reardon, *House Advances Federal Privacy Legislation*, CNET (July 21, 2022, 9:08 AM), https://www.cnet.com/news/privacy/house-advances-federal-privacy-legislation/ (citing American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022)).

318. H.R. 8152.

319. *Id.* § 2(8)(A).

320. *Federal Privacy Legislation—An Imminent Reality or Much Ado About Nothing?*, FISHER PHILLIPS (Aug. 4, 2022), https://www.fisherphillips.com/news-insights/federal-privacy-legislation-imminent-reality.html.

321. Emily Catron & Gary Kibel, *Federal Data Privacy Legislation: Differences with State Laws Raise Preemption Issues*, REUTERS, https://www.reuters.com/legal/legalindustry/federal-data-privacy-legislation-differences-with-state-laws-raise-preemption-2022-08-10/ (Aug. 10, 2022, 10:19 AM) ("Large [d]ata [h]olders [are] covered entities with over $250 million in gross annual revenue that process [c]overed [d]ata of more than five million individuals, or [s]ensitive [d]ata of 200,000 individuals, annually."); *see also* H.R. 8152 §§ 2(7), 207(c)(1)(A).

322. H.R. 8152 §§ 205(a)–(b), 2(11).

323. *Id.* §§ 401, 403.

would preempt most state privacy laws, including California's, which is stronger in some respects.[324]

The ADPPA would replace the current patchwork of state laws with national standards.[325] It would also extend new protections to residents of states that do not have their own regulatory framework.[326] Its provisions could force major data-collecting companies, such as Meta, Google, and Apple, to significantly change their business model.[327]

However, even if the ADPPA were to be enacted, it would leave gaps in the protection of data maintained by DTC genomic and neurotechnology testing companies. These companies would still be able to share data with third parties, which as data recipients rather than data collectors, are not subject to the same restrictions.[328] Moreover, many customers might not be aware of the protections afforded by the law, and it would provide little protection for relatives, acquaintances and others who are identified by the data.[329]

---

324. *Compare id.* (setting forth limitations on government entities' receiving of personal data, as well as a private right of action to obtain *monetary compensation*) *with* CAL. CIV. CODE §§ 1798.100–1798.199.100 (setting forth no such provisions, while also allowing several exemptions to data collection protections); *see also* Mark Stone, *California v. Congress: Data Protection Law Showdown*, SECURITYINTELLIGENCE (Jan. 6, 2023), https://securityintelligence.com/articles/california-cpra-congress-adppa-data-protection-law/.

325. *See The American Data Privacy and Protection Act*, A.B.A. (Aug. 30, 2022), https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl/; *see also* DANIEL CASTRO, LUKE DASCOLI & GILLIAN DIEBOLD, THE LOOMING COST OF A PATCHWORK OF STATE PRIVACY LAWS 1 (2022), https://www2.itif.org/2022-state-privacy-laws.pdf.

326. *See* Joseph Duball, *State Views on Proposed ADPPA Preemption Come into Focus*, IAPP (Sept. 27, 2022), https://iapp.org/news/a/state-level-views-on-proposed-adppa-preemption-come-into-focus/.

327. *See* Reardon, *supra* note 317.

328. *See also* JONATHAN M. GAFFNEY, CHRIS D. LINEBAUGH & ERIC N. HOLMES, CONG. RSCH. SERV., OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT 2, H.R. 8152 (2022); Stone, *supra* note 324.

329. *See* Mikolaj Barczentewicz, *ADPPA Mimics GDPR's Flaws, and Goes Further Still*, TRUTH ON THE MKT. (June 22, 2022), https://truthonthemarket.com/2022/06/22/adppa-mimics-gdprs-flaws-and-goes-further-still/; *supra* notes 318–23; Mark Wilson, *Most People Don't Understand Privacy, and That's a Huge Opportunity for Design*, FASTCOMPANY (Oct. 9, 2019), https://www.fastcompany.com/90414691/most-people-dont-understand-privacy-and-thats-a-huge-opportunity-for-design.

Additional measures to impose tighter regulation of DTC databases could take several forms. As a first step, mandated standardization of TOS would avoid the wide variation in policies that currently exists. Companies could be required to include clear privacy policies in their TOS that are prominently displayed on their websites and explained in simple English. Customers could then rely on certain basic protections regardless of which company they use.

Regulations governing TOS could also require companies to include various disclosures, statements of consumer rights, and commitments to adhere to stringent data protection practices. Disclosures would include the location where data are stored, the people who are authorized to access them, and the people and organizations with which data can be shared. For brain data whose collection is exempt from FDA approval, companies could be required to disclose the lack of that approval and the lack of clinical trials to determine effectiveness and risks. Consumer rights would include access to data, correction of errors, data deletion, and prohibition of data transfer. Stringent data protection practices could include use of rigorous anonymization techniques, prompt notification of data breaches, and use of encryption.

More rigorous regulatory schemes are also possible. A proposal for oversight of all DTC genomic data arrangements with external entities has been proposed by this author and colleagues.[330] The oversight would involve review boards known as Data Protection Review Boards (DPRBs) that are similar to IRBs.[331] Members of the boards would review data security arrangements whenever a company permits a third party to access the data that it maintains.[332] Among the elements that DPRBs would require would be data encryption, limits on personnel authorized to access them, and data deletion after a

330. *See* Robert I. Field, Anthony W. Orland & Arnold J. Rosoff, *Am I My Cousin's Keeper? A Proposal to Protect Relatives of Genetic Database Subjects*, 18 IND. HEALTH L. REV. 1, 1–3 (2021).

331. *See id.* at 2.

332. *See id.*

project has been completed.[333] The boards would also consider safeguards for identifiable relatives of data subjects.[334] Establishment and operation of the boards would be overseen by the FTC with an infusion of additional resources or by a new agency.[335]

Similar review boards could oversee data sharing arrangements for DTC companies that maintain brain data. The need for oversight of these companies is arguably more compelling than for genomic data companies because of the possibility of covert manipulation of subjects, for example with subliminal images as in the Flappy Whale experiment.[336] Review boards would add substantially greater assurance of subject protection, as IRBs do for other kinds of human subjects research.[337]

Whatever form of regulation is added, there is a need for international harmonization, since the collection, use, and maintenance of data are global.[338] A disjointed legal environment makes compliance by data collectors difficult and can even threaten national economic development.[339] It is especially important that the United States coordinate whatever reforms it implements with the EU and countries that have substantial technology sectors, such as China and India. In addition to easing the burden of compliance, this would provide more uniform protection for data subjects. However, there is a special challenge that must be taken into account for

333. *See id.* at 51–52.

334. *Id.* at 47, 51.

335. *See id.* at 47–48.

336. *See supra* Section I.B. (describing the Flappy Whale experiment).

337. *See* Field, *supra* note 330, at 37.

338. *See generally* Robert L. Totterdale, *Globalization and Data Privacy: An Exploratory Study*, 4 INT'L J. INFO. SEC. & PRIV. 19, 19–34 (2010) (surveying privacy laws across the world as well as the aggregation, retention, development, and movement of data by companies and other actors in the global privacy framework).

339. *See* Michael Pisa & Ugonma Nwankwo, *Are Current Models of Data Protection Fit for Purpose? Understanding the Consequences for Economic Development*, CTR. FOR GLOB. DEV., Aug. 2021, at 1, 6–7, https://cgdev.org/sites/default/files/are-current-models-data-protection-fit-purpose-understanding-consequences-economic.pdf.

low and middle-incomes countries that face resource constraints in implementing regulatory schemes.[340]

CONCLUSION

While the risks to privacy and the need for stronger legal protections are real, individual protection from unauthorized disclosure of genetic and brain data must be balanced against the need to foster innovation. Excessive regulation could stunt the growth of genomic medicine and neurotechnology techniques that hold the promise of preventing vast amounts of suffering and saving countless lives.[341] The conflict calls for a careful balance between public protection and legal reform.

Achieving that balance will not be easy as it must resolve a clash between a fundamental human right and powerful commercial interests. Some commentators have expressed concern that the legal system is not equipped to resolve it.[342] However, in addition to leaving millions of people vulnerable to harm, failure to find a viable balance could jeopardize the biomedical research enterprise itself.[343] If the collection of sensitive biometric information that can be stored indefinitely makes people reluctant to use services that collect their data, much of the fuel that powers innovation could be lost.[344]

340. *See id.* at 7.

341. *See* James P. Evans & Michael S. Watson, *Genetic Testing and FDA Regulation: Overregulation Threatens the Emergence of Genomic Medicine,* 313 JAMA 669, 669–70 (2015).

342. *See, e.g.*, Kuner et al., *supra* note 182, at 141–42.

343. *See* Laura Hautala, *Genetic Testing Hampered by Data Privacy Concerns, Experts Say*, CNET (Feb. 26, 2020, 11:45 AM), https://www.cnet.com/news/privacy/genetic-testing-hampered-by-data-privacy-concerns-experts-say/; Venky Anant, Lisa Donchak, James Kaplan & Henning Soller, *The Consumer-Data Opportunity and the Privacy Imperative*, MCKINSEY & CO., Apr. 2020, at 1, 2, https://www.mckinsey.com/~/media/mckinsey/business%20functions/risk/our%20insights/the%20consumer%20data%20opportunity%20and%20the%20privacy%20imperative/the-consumer-data-opportunity-and-the-privacy-imperative.pdf ("The scale of consumer data exposed in the most catastrophic breaches is staggering. In two breaches at one large corporation, more than 3.5 billion records were made public. Breaches at several others exposed hundreds of millions of records.").

344. *See* Hautala, *supra* note 343.

Genomic research brought not only new possibilities but also new risks in the collection of sensitive personal information.[345] Neurotechnology has added another layer in both regards. Awareness of the risks and of gaps in existing legal protections is a first step. Designing regulatory remedies that can be applied on a global basis should be the next step. Such remedies will be an essential part of unleashing the full potential of genomics and neurotechnology, two engines of innovation that hold so much promise.

345. *See supra* Part I.