Consumer Health Data Privacy & Security

A State-Level Scan

June 2024

Background

Consumer Health Technologies

About one in three Americans use consumer health technologies, which includes wearable devices (e.g., wrist-worn fitness trackers or smartwatches) and third-party health and wellness applications (e.g., fertility trackers).[1] These technologies present unique pathways to help consumers better manage their health and wellbeing through real-time monitoring of biometric data and lifestyle factors, such as glucose levels, UVA exposure, heart rate, blood pressure, body temperature, oxygen saturation, and physical activity.[2] This information helps companies provide personalized services to consumers from tracking health and fitness status, predicting the likelihood of a potential health event (e.g., heart attack), and sending automated health reminders and educational prompts.[3, 4] Consumer health technologies also provide opportunities to monitor health and wellness beyond hospital and ambulatory care settings, particularly in more rural areas and other communities with access to fewer health resources.[5]

Existing Federal Privacy and Security Protections

Federal rules provide a floor for health data privacy and security. The Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act, applies to health information that is created, stored, maintained, or transmitted by HIPAA-covered entities[6] and their business associates.[7] HIPAA protections must be in place when data generated through consumer health technologies are sent to a health care practice's electronic health record system; HIPAA does not always apply when such technologies are used for personal use. The Federal Trade Commission Act (Act)[8] applies to both HIPAA-covered entities and business associates, as well as non-covered entities offering technology and services that collect, use, and share consumer health data.[9] This includes developers of mobile health applications, personal health devices, and genetic information services and products.[10] The Act tasks the Federal Trade Commission with protecting the public from fraudulent, deceptive, and unfair practices in or affecting commerce; this includes making sure businesses take reasonable steps to protect and secure health information from unauthorized use or disclosure.[11, 12]

Scan Overview

The Maryland Health Care Commission (MHCC) conducted a legislative scan (scan) to identify states with consumer data privacy laws that aim to enhance consumer protections.[13] In general, states have

enacted more stringent laws to close gaps in protections for health data that are not covered under federal rules, particularly in the wake of the Dobbs v. Jackson Women's Health Organization ruling (2022).[14] As of 2024, a total of 26 states, including Maryland, have passed legislation, an increase of 18 states since 2021. **Table 1** provides a high-level snapshot of comprehensive data privacy laws, including key categories regarding consumer rights and business obligations. **Table 2** provides detailed information on laws (new and recently amended) that are specific to consumer health data or certain types of health information (e.g., mental health, reproductive health). **Table 3** highlights state laws that establish protections for data generated through direct-to-consumer genetic testing companies.[15]

Scan findings are based on publicly available information and highlight certain provisions of legislation enacted by states; refer to state-specific laws for more detailed information.

Comprehensive Consumer Data Privacy Laws

Twenty states have comprehensive data privacy laws[16] which give consumers the right to know how and with whom their data is used, shared, or sold, as well as the right to opt-in, opt-out, and/or restrict the selling and sharing of their personal information. California was the first state to pass legislation in 2018 (i.e., California Consumer Privacy Act or CCPA). Since then, momentum has increased among states to enact legislation – 2021 (CO, VA), 2022 (CT, UT), 2023 (DE, IA, IN, MT, OR, TN, TX), and 2024 (KY, MD, MN, NE, NH, NJ, RI). These laws require businesses that process[17] personal information to clearly state in a privacy notice the categories of data collected, how the data is used, and if data are shared with third parties (e.g., data brokers).[18] Maryland is the only state to restrict data collection to only what is reasonably necessary to provide or maintain a product or service requested by a consumer.[19]

Some states require opt-in consent before businesses can process personal information categorized as "sensitive" (definitions vary by state).[20] Maryland defines sensitive data as "any data related to an individual's health, ethnicity and religion along with biometric data, geolocation data and data belonging to a known minor under age 18." Maryland is the only state to ban the sale of such data from individuals of any age.[21] Some states require businesses to implement certain security safeguards (e.g., conduct regular risk assessments) or recognize universal opt-out mechanisms.[22, 23] Applicability varies from state to state with some laws including small to mid-sized businesses while others are limited to larger technology companies, such as Amazon, Google, Apple, and Facebook.

Consumer advocacy organizations like the Electronic Privacy Information Center and U.S. PIRG Education Fund believe privacy laws among states do not offer adequate consumer protections.[24] For example, most laws require companies to be transparent about data collection and use in their privacy policies, but readability and understanding of those policies can be difficult.[25] In addition, many states that give consumers the right to request their data be deleted require consumers to submit such requests to individual companies; this is generally viewed as impractical given the number of companies that collect information about consumers via mobile applications and websites.[26] California passed a law in 2023 requiring the development of a centralized process by January 2026 for consumers to submit a single deletion request to data brokers registered in the state (approximately 500).[27, 28]

Table 1: Consumer Data Privacy Laws 20 States							
General Information	**Consumer Privacy Rights**					**Business Obligations**	
State/Statute	**Portability[29]**	**Correct**	**Delete**	**Opt-Out Sales[30]**	**Opt-In Sensitive Data Processing[31]**	**Security Risk Assessments**	**Universal Opt-Out Mechanism**
California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA) CCPA: Enacted 2018 | Effective 1/1/20 CPRA: Enacted 2020 | Effective 1/1/23	✓	✓	✓	✓		✓	✓
Colorado Privacy Act Enacted 2021 | Effective 7/1/23	✓	✓	✓	✓	✓	✓	✓
Connecticut Data Privacy Act Enacted 2022 | Effective 7/1/23	✓	✓	✓	✓	✓	✓	✓
Delaware Personal Data Privacy Act Enacted 2023| Effective 1/1/25	✓	✓	✓	✓		✓	✓
Florida Digital Bill of Rights Enacted 2023 | Effective 7/1/24	✓	✓	✓	✓	✓		
Indiana Consumer Data Protection Act Enacted 2023 | Effective 1/1/26	✓	✓	✓	✓	✓	✓	
Iowa Consumer Data Protection Act Enacted 2023 | Effective 10/1/25		✓		✓			
Kentucky Consumer Data Protection Act Enacted 2024 | Effective 1/1/26	✓	✓	✓	✓	✓	✓	✓
Maryland Online Data Privacy Act of 2024 Enacted 2024 | Effective 10/1/25	✓	✓	✓	✓	✓	✓	✓
Minnesota Consumer Data Privacy Act Enacted 2024 | Effective 7/31/25	✓	✓	✓	✓	✓	✓	✓
Montana Consumer Data Privacy Act Enacted 2023 | Effective 10/1/24	✓	✓	✓	✓	✓	✓	✓
Nebraska Data Privacy Act Enacted 2024 | Effective 1/1/25	✓	✓	✓	✓	✓	✓	
New Hampshire Expectation of Privacy Act Enacted 2024 | Effective 1/1/25	✓	✓	✓	✓	✓	✓	✓
New Jersey Data Privacy Act Enacted 2024 | Effective 1/15/25	✓	✓	✓	✓	✓	✓	✓

Table 1: Consumer Data Privacy Laws 20 States							
General Information	**Consumer Privacy Rights**					**Business Obligations**	
State/Statute	**Portability[29]**	**Correct**	**Delete**	**Opt-Out Sales[30]**	**Opt-In Sensitive Data Processing[31]**	**Security Risk Assessments**	**Universal Opt-Out Mechanism**
Oregon Consumer Privacy Act Enacted 2023 |Effective 7/1/24	✓	✓	✓	✓	✓	✓	✓
Rhode Island Data Transparency & Privacy Protection Act Enacted 2024 | Effective 1/1/25	✓	✓	✓	✓	✓	✓	
Tennessee Information Protection Act Enacted 2023 | Effective 7/1/25	✓	✓	✓	✓	✓	✓	
Texas Data Privacy and Security Act Enacted 2023 | Effective 7/1/24	✓	✓	✓	✓	✓	✓	✓
Utah Consumer Privacy Act* Enacted 2022| Effective 12/31/23	✓		✓	✓			
Virginia Consumer Data Protection Act* Enacted 2021 | Effective 1/1/23	✓	✓	✓	✓	✓	✓	

Laws Specific to Consumer Health Data

In 2022 and 2023, California passed amendments to the California Confidentiality of Medical Information Act (CMIA). The changes designate consumer health apps that collect information about mental health data (e.g., online therapy apps) or sexual and reproductive health information (e.g., fertility trackers) as health care providers subject to CMIA provisions. In 2023, Washington and Nevada passed laws aimed at protecting consumer health data that falls outside the bounds of HIPAA, including personal information that can be linked to an individual's past, present, or future physical or mental health status. This includes information (e.g., internet search activity, purchase history) that indicates a consumer's attempt to acquire or receive certain health services or supplies or infer a consumer's health status.

States have strengthened protections for consumer health data related to reproductive or sexual health after the Supreme Court's decision in 2022 that returned power to individual states to regulate any aspect of abortion not protected by federal law.[32, 33] Some states have amended legislation to carve out protections for certain data in part due to heightened concerns involving access to records of individuals seeking reproductive health care.[34] Five states prohibit the use of geofencing (i.e., a type of location-based service used for marketing and advertising)[35] within a specified distance of reproductive health

centers and other health care facilities (CT, MD, NV, NY, WA). Connecticut amended its data privacy law to include opt-in consent for any collection, use, disclosure, sale, or processing of consumer health data with specific mention of information related to sexual or reproductive health and gender-affirming care. California clarified provisions in the CCPA that allow businesses to disclose personal information to government agencies under certain circumstances (e.g., a person is at risk of death or serious injury).

Table 2: Laws/Amendments Specific to Consumer Health Data
5 States

State/Statute	Applicability	Key Provisions
California - Privacy: Mental Health Digital Services: Mental Health Application Information Amends Confidentiality of Medical Information Act (CMIA) Enacted 2022 Effective 9/28/22	Any business that offers a mental health digital service to a consumer for the purpose of allowing the individual to manage the individual's information, or for the diagnosis, treatment, or management of a medical condition (e.g., a health and wellness app that asks users to record anxiety symptoms)	• Deems businesses that provide digital mental health as health care providers for purposes of the CMIA and thus subject to provisions in CMIA • CMIA prohibits health care providers from sharing, selling, using for marketing, or otherwise using any medical information for purposes not necessary to provide health care services without the consumer's signed authorization • Businesses that partner with health care providers (e.g., licensed mental health therapists) must disclose to the providers information regarding how to find data breaches reported to the Attorney General pursuant to Section 1798.82
California Confidentiality of Medical Information Act: Reproductive or Sexual Health Application Information Amends Confidentiality of Medical Information Act (CMIA) Enacted 2023 Effective 1/1/24	Businesses in California that offer a reproductive or sexual health digital service to a consumer, including mobile-based applications and internet websites	• Deems business that offer reproductive or sexual health digital services as health care providers for purposes of the CMIA and thus subject to provisions in CMIA ○ CMIA prohibits health care providers from sharing, selling, using for marketing, or otherwise using any medical information, including reproductive or sexual health application information, for purposes not necessary to provide health care services without the consumer's signed authorization
AB-1194 California Privacy Rights Act of 2020: exemptions: abortion services Enacted 2023 Effective 1/1/24 Amends California Consumer Privacy Act (CCPA) as amended by the California Privacy Rights Act (CPRA)	CCPA as amended by CPRA applies to business that meet one of the following: • Has annual gross revenues of at least $25 million per year • Buys, sells, shares, or receives personal information from at least 100,000 California consumers or household for commercial purposes • Earns at least half of its annual gross revenues per year from selling or sharing California consumers' personal information	• Makes clarifications to the "Emergency Access" provisions in the CCPA as amended by the CPRA (i.e., California's comprehensive consumer data privacy law) that permits businesses to disclose a consumer's personal information to government agencies under certain circumstances ○ Clarifies that a consumer accessing, procuring, or searching for services regarding contraception, pregnancy care, and prenatal care, including, but not limited to, abortion services, does not constitute a natural person being at risk or danger of death or serious physical injury

Table 2: Laws/Amendments Specific to Consumer Health Data 5 States		
State/Statute	**Applicability**	**Key Provisions**
Connecticut S.B. 3 Enacted 2023 Effective 10/1/23 Amends **Connecticut Data Privacy Act**	People who conduct business in Connecticut or who produce products or services targeted to Connecticut residents and that, during the prior calendar year, controlled or processed the personal data of at least 100,000 consumers or 25,000 or more consumers, and derived over 25% of gross revenue from the sale of personal data	• Defines "consumer health data" as any personal data that a business uses to identify a consumer's physical or mental health condition or diagnosis, including, but not limited to, gender-affirming, reproductive, and sexual health data • Requires clear and affirmative (opt-in) consent for any collection, use, disclosure, sale or other processing of consumer health data • Prohibits geofencing within 1,750 feet of any mental, reproductive, or sexual health facility for the purpose of "identifying, tracking, collecting data from or sending any notification to a consumer regarding that consumer's health data"

Nevada's Consumer Health Data Privacy Law
 	
Enacted 2023
Effective 3/31/24
	Any "regulated entity" that conducts business in Nevada or produces or provides products or services that are targeted to consumers in Nevada and determines the purpose and means of processing, sharing, or selling consumer health data	• Grants consumers the right to access, delete and withdraw consent regarding health data
		• Regulated entities must obtain consent to collect, share or sell consumer health data and maintain policies and practices for the administrative, technical, and physical security of consumer health data
		• Prohibits a person from geofencing within 1,750 feet of any person or entity that provides in-person health care services or products for the following purposes:
		  ○ Identifying or tracking consumers seeking in-person health care services or products
		  ○ Collecting consumer health data
		  ○ Sending notifications, messages, or advertisements to consumers related to their consumer health data or health care services or products

New York State Assembly Bill 2023-A3007C Enacted 2023 Effective 7/2/23 Amends **General Business Law section 394-g**	Any person, corporation, partnership, or association	• Prohibits any person, corporation, partnership, or association from geofencing around any health care facility they do not own for the purpose of advertising, building a consumer profile, or to infer the health status, medical condition, or medical treatment of any person at or within a health care facility

Table 2: Laws/Amendments Specific to Consumer Health Data 5 States		
State/Statute	**Applicability**	**Key Provisions**
Washinton My Health My Data Act Enacted 2023 | Effective 3/31/24	Any legal entity that conducts business in the state or targets products or services to Washington consumers and determines the purpose and means of collecting, processing, sharing or selling consumer health data *Government agencies, tribal nations and contracted service providers that process consumer health data on behalf of government agencies are not included in the scope of the law*	• Grants consumers the right to access, delete and withdraw consent regarding health data, requires regulated entities and small businesses to obtain consent to collect, share or sell consumer health data, and makes violations enforceable under the Consumer Protection Act which includes a private right of action • Defines Consumer Health Data broadly as: "personal information that is linked or reasonably linkable to a consumer and that identifies the consumer's past, present or future physical or mental health status" • Includes non-health data when used to identify a consumer's health status through inferences, proxies or algorithms • Makes it unlawful for any actual or legal person to utilize a geofence around an entity that provides in-person health care services and identify or track consumers seeking health services, collect health data from consumers, or send notifications, messages or ads to consumers related to their health data or services received

Genetic Data Privacy Laws

Twelve states have laws that include protections for genetic data generated using test kits sold directly to consumers. These kits offer services that make determinations about a consumer's general health, disease risk, and ancestry.[36] Most states, including Maryland, use model legislation based on best practices published by the Future of Privacy Forum, a think tank and advocacy group focused on advancing responsible data practices.[37, 38] These laws generally prohibit companies from sharing genetic information with insurers, give consumer rights around accessing and deleting their personal information, and allow consumers to request that their genetic sample be destroyed. The laws also require express consent from the consumer before companies can use genetic data for marketing, research, and other third-party sharing.[39] Florida and South Dakota prohibit the disclosure of genetic data to insurers; statutory requirements do not extend to consumer rights.[40]

Table 3: Genetic Data Privacy Laws 12 States
Arizona Genetic Information Privacy Act (GIPA) Enacted 2021 | Effective 9/29/21
California Genetic Information Privacy Act (GIPA) Enacted 2021 | Effective 1/1/22
Florida Protecting DNA Privacy Act Enacted 2021 | Effective 10/1/21
Florida Genetic Information for Insurance Purposes Enacted 2020 | Effective 7/1/2020
Kentucky Genetic Information Privacy Act Enacted 2022 | Effective 6/1/22
Maryland Genetic Information Privacy Act Enacted 2022 | Effective 10/1/22
Montana Genetic Information Privacy Act Enacted 2023 | Effective 7/1/23
South Dakota Genetic Information Privacy Act Enacted 2021 | Effective 7/1/23
Tennessee Genetic Information Privacy Act Enacted 2023 | Effective 7/1/23
Texas Genetic Privacy Act Enacted 2023 | Effective 9/1/23
Utah Genetic Information Privacy Act (GIPA) Enacted 2022 | Effective 5/5/21
Virginia Genetic Data Privacy Law Enacted 2023 | Effective 7/1/23
Wyoming Genetic Information Privacy Act Enacted 2022 | Effective 7/1/22

Looking Forward

The consumer data privacy landscape will continue to evolve absent a federal framework that applies across sectors (e.g., health care, education, finance).[41] Many states recognize the need to consider legislation in ways that keep pace with advances in consumer health technologies and give consumers more choice over how companies acquire and utilize their personal data beyond HIPAA. Ensuring consumer confidence and trust requires strong privacy and security protections and greater consumer transparency of data handling practices.

The document is not exhaustive of the consumer data privacy landscape and should not be construed as legal advice. For questions, contact Kelly Scott at kelly.scott@maryland.gov.

Endnotes

[1] National Heart, Lung, and Blood Institute, *Study Reveals Wearable Device Trends Among U.S. Adults*, June 2023. Available at: www.nhlbi.nih.gov/news/2023/study-reveals-wearable-device-trends-among-us-adults#:~:text=Almost%20one%20in%20three%20Americans,Health%20Information%20National%20Trends%20Survey.
[2]MedCity News, *How Wearable Devices Empower Healthcare Providers*, July 2021. Available at: medcitynews.com/2021/07/how-wearable-devices-empower-healthcare-providers/.
[3] Lavallee DC, Lee JR, Austin E, Bloch R, Lawrence SO, McCall D, Munson SA, Nery-Hurwit MB, Amtmann D. *mHealth and patient generated health data: stakeholder perspectives on opportunities and barriers for transforming healthcare*. Mhealth. 2020 Jan 5;6:8. doi: 10.21037/mhealth.2019.09.17. PMID: 32190619; PMCID: PMC7063266.
[4] Lawrence K. Digital Health Equity. In: Linwood SL, editor. Digital Health [Internet]. Brisbane (AU): Exon Publications; 2022 Apr 29. Chapter 9. Available at: www.ncbi.nlm.nih.gov/books/NBK580635/ doi: 10.36255/exon-publications-digital-health-health-equity.
[5] Fraser MJ, Gorely T, O'Malley C, Muggeridge DJ, Giggins OM, Crabtree DR. *Does Connected Health Technology Improve Health-Related Outcomes in Rural Cardiac Populations? Systematic Review Narrative Synthesis.* International Journal of Environmental Research and Public Health. 2022; 19(4):2302. doi.org/10.3390/ijerph19042302.
[6] Covered entities include health plans, health care clearinghouses, health care providers, and business associates.
[7] Business Associates include entities that create, receive, maintain, or transmit protected health information entities or another business associate.
[8] The Federal Trade Commission (FTC) was created on September 26, 1914 when President Woodrow Wilson signed the Federal Trade Commission Act into law. More information is available at: www.ftc.gov.
[9] For purposes of this scan, consumer health data is information that is linked or can be reasonably linked to a consumer that identifies past, present, or future physical or mental health status and is not protected by HIPAA.
[10] U.S. Department of Health and Human Services, National Committee on Vital and Health Statistics, *Health Information Privacy Beyond HIPAA: A Framework for Use and Protection*, June 2019. Available at: ncvhs.hhs.gov/wp-content/uploads/2019/07/Report-Framework-for-Health-Information-Privacy.pdf.
[11] The FTC Health Breach Notification Rule requires companies that experience a breach of security of consumers' identifying health information to notify affected consumers, the FTC, and, in some cases, the media.
[12] U.S. Department of Health and Human Services, *Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule*, September 2023. Available at: www.hhs.gov/hipaa/for-professionals/special-topics/hipaa-ftc-act/index.html.
[13] This legislative scan is an update of previous legislative scans completed in 2021 and 2022.
[14] National Constitution Center, *Dobbs v. Jackson Women's Health Organization (2022)*. Available at: constitutioncenter.org/the-constitution/supreme-court-case-library/dobbs-v-jackson-womens-health-organization.
[15] Direct-to-consumer genetic testing companies generally request the consumer collect a specimen, such as saliva or urine, and send it to the company for testing and analysis of their DNA (or genome). Results are used for a variety of purposes, such as predicting risk of developing certain diseases, identifying potential medication or diet intolerances, and exploring genetic ancestry. More information is available at: www.fda.gov/medical-devices/in-vitro-diagnostics/direct-consumer-tests.
[16] Consumer data privacy laws are considered comprehensive if they carry omnibus sets of consumer rights and business obligations and apply to broad ranges of entities. More information is available at: iapp.org/resources/article/us-state-privacy-laws-overview/.
[17] "Data processing" includes collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data.
[18] Data brokers collect and sell or license the data of consumers with whom they do not have a direct relationship, usually for advertising and marketing purposes.
[19] JDSupra, *Maryland Legislature Passes Consumer Data Privacy Bill*, April 2024. Available at: www.jdsupra.com/legalnews/maryland-legislature-passes-consumer-6185962/.
[20] Greenberg Traurig, *Update: Processing Sensitive Personal Information under U.S. State Privacy Laws,* September 2023. Available at: www.gtlaw-dataprivacydish.com/2023/09/update-processing-sensitive-personal-information-under-u-s-state-privacy-laws/.
[21] Future of Privacy Forum, *Peak Privacy: Vermont's Summit on Data Privacy*, May 2024. Available at: fpf.org/blog/peak-privacy-vermonts-summit-on-data-privacy/.
[22] Universal Opt-Out Mechanisms (UOOMs) refer to a range of online tools that allow consumers to configure their devices to automatically opt out of the sale or sharing of their personal information with internet-based entities with whom they interact. These tools transmit consumers' opt-out preferences by using technical specifications, such as the Global Privacy Control (GPC). More information is available at: fpf.org/blog/survey-of-current-universal-opt-out-mechanisms/.
[23] Maryland is the only state that includes language around UOOMs but makes the recognition of opt-out preference signals optional rather than mandatory by a specified date.

[24] Several state data privacy laws were based on Virginia Consumer Data Protection Act ,which was initially drafted by an Amazon lobbyist and allows companies to collect any data for any reason as long as it is disclosed somewhere in a privacy policy. More information is available at: pirg.org/edfund/wp-content/uploads/2024/01/State-of-Privacy-Feb.-2024.pdf.
[25] University of Pennsylvania, Annenberg School for Communication, *Americans Can't Consent to Companies' Use of Their Data*, February 2023. Available at: www.asc.upenn.edu/sites/default/files/2023-02/Americans_Can%27t_Consent.pdf.
[26] Electronic Privacy Information Center and Public Interest Research Group, *The State of Privacy*, February 2024. Available at: pirg.org/edfund/wp-content/uploads/2024/01/State-of-Privacy-Feb.-2024.pdf.
[27] The Delete Act requires the California Privacy Protection Agency to develop a centralized process by January 1, 2026 for consumers to request their personal information be deleted by all data brokers registered in California. More information is available at: iapp.org/news/a/california-governor-signs-ca-delete-act-into-law/.
[28] California Civil Code § 1798.99.80 requires data brokers to register with the California Privacy Protection Agency on its website by January 31, 2024 and every subsequent year in which a business meets the definition of a data broker. More information is available at: cppa.ca.gov/data_brokers/.
[29] Refers to the right for a consumer to request their personal information be shared in a common file format.
[30] Refers to the right for a consumer to opt out of the sale of their personal information to third parties.
[31] Refers to the right for a consumer to give opt-in consent before businesses can process personal information categorized as "sensitive personal information"; definitions of sensitive personal information vary by state but generally includes health information or certain types of health information (e.g., mental health, genetic data).
[32] See n. 14, *Supra.*
[33] Bloomberg Law, *Abortion-Rights States Begin Shielding Digital Data Near Clinics*, January 2023. Available at: news.bloomberglaw.com/privacy-and-data-security/abortion-rights-states-begin-shielding-digital-data-near-clinics.
[34] The Office of Governor Gavin Newsom, *Letter to the California State Assembly*, October 2023. www.gov.ca.gov/wp-content/uploads/2023/10/AB-1194-SIGN-MSG-1.pdf.
[35] Geofencing involves setting up a virtual perimeter around a specific real-world zone or location to deliver advertisements to specific zip codes, Wi-Fi or IP addresses, or to a certain event (e.g., concert, conference) by using GPS. More information is available at: www.jdsupra.com/legalnews/new-york-and-connecticut-prohibit-5994948/.
[36] Moscarello, Tia & Murray, Brittney & Reuter, Chloe & Demo, Erin. (2018). Direct-to-consumer raw genetic data and third-party interpretation services: more burden than bargain? Genetics in Medicine. 21. 10.1038/s41436-018-0097-2.
[37] Best practices were established in collaboration with leading direct-to consumer genetic testing companies (e.g., Ancestry, 23 and Me). The report is available at: fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf.
[38] Future of Privacy Forum, *DNA of Genetic Privacy Legislation: Montana, Tennessee, Texas, and Virginia Enter 2024 with New Genetic Privacy Laws Incorporating FPF's Best Practices*, March 2024. Available at: fpf.org/blog/the-dna-of-genetic-privacy-legislation-montana-tennessee-texas-and-virginia-enter-2024-with-new-genetic-privacy-laws-incorporating-fpfs-best-practices/.
[39] *Ibid.*
[40] Florida passed a law in 2021 making it illegal (second-degree felony) for companies to sell or transfer genetic data to a third-party without express consent. In Florida, second-degree felonies are punishable by up to 15 years in prison, 15 years of probation, and a $10,000 fine.
[41] IAPP, Filling the Void? *The 2023 State Privacy Laws and Consumer Health Data*, March 2023. Available at: iapp.org/news/a/filling-the-void-the-2023-state-privacy-laws-and-consumer-health-data/.