Loyola Consumer Law Review

Volume 34 | Issue 1 Article 7

2022

Consumer News: Fertility Tracking Apps, DNA Testing, and... Vending Machines? Developments In FTC and State Protections On Certain Health Information

Kiana Baharloo

CONSUMER NEWS: FERTILITY TRACKING APPS, DNA TESTING, AND... VENDING MACHINES?

DEVELOPMENTS IN FTC AND STATE PROTECTIONS ON CERTAIN HEALTH INFORMATION

Kiana Baharloo, News Editor

I. BACKGROUND

Given the segmented nature of privacy laws and regulations in the United States,[1] certain electronic health information has fallen through the cracks of specific regulations, rendering consumers' data vulnerable to privacy and security concerns.[2] Specifically, Internet-connected health devices, applications ("apps"), and accompanying technologies, often referred to as the Internet of Medical Things ("Medical IoT" or "IoMT"), generate serious privacy concerns for consumers.[3] The Federal Trade Commission ("FTC") recognizes the "proliferation of apps and connected devices that capture sensitive health data" caused by an "explosion in health apps" that allow consumers to "track diseases, diagnoses, treatment, medications, fitness, fertility, sleep, mental health, diet, and other vital areas."[4] The FTC

---

[1] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, NY TIMES (Sept. 16, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.

[2] *Statement of the Commission on Breaches by Health Apps and Other Connected Devices,* FED. TRADE COMM'N, https://www.ftc.gov/system/files/documents/rules/health-breach-notification-rule/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf (last visited Dec. 20, 2021).

[3] Bandar Alamri, et al., *Preserving Patients' Privacy in Medical IoT Using Blockchain*, 12407 EDGE COMPUTING Lecture Notes in Computer Science (2020).

[4] *Statement of the Commission*, *supra* note 2.

clarified that health information that is not covered by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") has been a "growing concern given the rise of autonomy and health awareness in recent years, especially as this trend has led to increased use of apps and other internet connected devices."[5] A distinct concern of the IoMT is that using large amounts of complex data ("big data"), certain consumer data, other than what the consumer input themselves, can be derived using "advanced statistical analysis and the cross-referencing of different sources of data."[6] Consumers do not have knowledge of the existence of such derived data, nor when it is breached.[7] HIPAA only regulates covered entities and a statutorily defined subset of information classified as "protected health information," which, in practice, is typically limited to information in the traditional medical field consisting of doctors, clinics, and insurance companies.[8] HIPAA does not cover "data generated by a myriad of people or products other than the patient" or "user-generated information about health," such as health or wellbeing apps, or "the huge volume of data that is not about health at all, but permits inferences about health."[9] Compartmentalization and separation of protected health information covered by HIPAA has left non-covered entities, especially those in the business of IoMT, with little accountability when faced with a data breach.[10]

There is currently no single controlling federal law covering health apps, genetic databases, or wearable devices, so consumer complaints are submitted to the FTC, as opposed to the Department of Health and Human Services or the Office of Civil Rights in a HIPAA complaint.[11] A critical flaw in the FTC's enforcement of this type of health information protection is that, due to lack of required breach notifications, consumers are typically unaware when there is a breach consisting of their personal information or if their information is sold or shared.[12] Because of this flaw, "there is no legal requirement for companies to implement updated and adequate privacy and data

---

[5] *Id.*

[6] Alda Yuan, *Derived Data: A Novel Privacy Concern in the Age of Advanced Biotechnology and Genome Sequencing*, 37 YALE L. & POL'Y REV., Aug. 2018, at 6-9.

[7] *Id.* at 2.

[8] *Covered Entities and Business Associates*, HEALTH & HUM. SERV., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Dec. 20, 2021).

[9] W. Nicholson Price II & I. Glenn Cohen, *Privacy in the Age of Medical Big Data*, 25 NAT. MED. 5, 37-43 (2019).

[10] *Statement of the Commission*, *supra* note 2.

[11] Kim Theodos & Scott Sittig, *Health Information Privacy Laws in the Digital Age: HIPAA Doesn't Apply*, PERSP. HEALTH INFO. MGMT., 2021 at 5.

[12] *Id.*

safeguards nor is there any recourse for companies that fail to adopt commercially reasonable privacy or security standards."[13] Federal breach notification laws exist by sector (e.g. HIPAA, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act),[14] and each state has its own breach notification law.[15] However, the FTC's Health Breach Notification Rule, which has recently been expanded in scope to include health technologies, recognizes the limited entities covered by HIPAA, and, in order to ameliorate this gap, "covers vendors of personal health records that contain individually identifiable health information created or received by health care providers."[16]

Like the IoMT, another area of personal health information that is not covered by HIPAA is direct-to-consumer genetic testing ("DTC-GT").[17] This is due in part to the fact that laws relating to genetic testing did not anticipate consumers' ability to do their own genetic testing at home, outside of a medical setting.[18] While genetic information is not federally protected for privacy concerns, it is protected for non-discrimination purposes granted under the Genetic Information Non-discrimination Act ("GINA")[19] and the Clinical Laboratory Improvement Amendments of 1988 ("CLIA"), which require certain standards for laboratory quality.[20] Genetic information held by DTC-GT companies, such as 23andMe, is typically self-regulated through often insufficient privacy policies that do not clearly outline how consumers' genetic information is stored or shared.[21] Genetic data is subject to concerning privacy attacks, such as using information derived from

---

[13] Celia Rosas, *The Future is Femtech: Privacy and Data Security Issues Surrounding Femtech Applications*, 15 HASTINGS BUS. L.J. 328, 319-341 (2019).

[14] GINA STEVENS, CONG. RSCH. SERV., R42475, DATA SECURITY BREACH NOTIFICATION LAWS (2012).

[15] National Conference of State Legislatures, *Security Breach Notification Laws*, NAT'L CONF. STATE LEGISLATURES, https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (last visited Dec. 2021).

[16] *Statement of the Commission*, *supra* note 2.

[17] Ellen Wright Clayton, et al., *The Law of Genetic Privacy: Applications, Implications, and Limitations*, 6 J.L. & BIOSCIENCES 11, 36 (2019).

[18] Jennifer A. Gniady, *Regulating Direct-to-Consumer Genetic Testing: Protecting the Consumer Without Quashing a Medical Revolution*, 76 FORDHAM L. REV. 2436, 2429-2475 (2008).

[19] Clayton et al., *supra* note 17, at 13.

[20] *Clinical Laboratory Improvement Amendments (CLIA)*, CTRS. DISEASE CONTROL, https://www.cdc.gov/clia/index.html (last visited Dec. 20, 2021).

[21] Clayton et al., *supra* note 17, at 17 (providing an example that half of the DTC-GT companies in a 2017 survey did not specify that consumer data would or could be shared with third parties).

DNA for "personal gain, blackmail, to alter evidence in the case of forensics to be used in the court of law or some other dubious reasons."[22] This lack of federal regulation leaves DTC-GT companies potentially liable for Section 5 FTC Act violations under unfair and deceptive practices[23] through the FTC's investigative, law enforcement, and rulemaking authorities.[24] However, this is of little help to consumers if they read and consent to the company's terms by opting in, among other contract law issues, such as if consumers do not read the privacy policy at all, or misunderstand the terms.[25] Consent to terms that do not meaningfully protect consumers' data poses a dilemma because it "legitimizes nearly any form of collection, use, or disclosure of personal data."[26] On the other hand, "paternalistic measures, such as making the choice for individuals, restrains their ability to consent" and denies consumers "the freedom to make choices."[27] Power differentials also create an inability to influence privacy outcomes, and information asymmetries create few opportunities for consumers to bargain and ultimately obtain their desired privacy interests.[28] Consumer consent also presents a problem as consumers often agree to terms that do not contain effectual security information, such as encryption, access limitation, administrative procedures for handling information, and other controls devised to protect information.[29] In addition, the FTC Act unfair and deceptive practices standard may not be met if a

---

[22] Abukari Mohammed Yakubu & Yi-Ping Phoebe Chen, *Ensuring Privacy and Security of Genomic Data and Functionalities*, 21 BRIEFINGS IN BIOINFORMATICS 514, 511-526 (2020).

[23] Elisa Jillson, *Selling Genetic Testing Kits? Read On.*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/blogs/business-blog/2019/03/selling-genetic-testing-kits-read (last visited Dec. 20, 2021).

[24] *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (last visited Dec. 20, 2021).

[25] Clayton et al., *supra* note 17, at 16.

[26] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARVARD L. REV. 1880, 1880-1903 (2013).

[27] *Id.* at 1894 (discussing the "consent dilemma" where "privacy regulation, however, risks becoming too paternalistic. Regulation that sidesteps consent denies people the freedom to make choices. The end result is that either people have choices that are not meaningful or people are denied choices altogether. Ironically, paternalistic regulation might limit people's freedom to choose in the name of enhancing their autonomy").

[28] Charlotte Tschider, *The Consent Myth: Improving Choice for Patients of the Future*, 96 WASH. U. L. REV. 1505, 1519 (2018).

[29] Clayton et al., *supra* note 17, at 6.

company has a vague or broad privacy policy that does not necessarily constitute a lie.[30]

HIPAA was "never intended to afford comprehensive health privacy protection,"[31] and the few alternative routes of consumer protection over health information in the IoMT highlight the United States' lack of proper comprehensive data privacy. Furthermore, expanding HIPAA to classify those in the business of the IoMT as HIPAA covered entities could deter innovation and slow the process of placing new products in the marketplace.[32] Online privacy poses concerns for consumers because consumer data has become a commodity. Consumers essentially "enter into blind bargains online where they trade their personal information for free websites and apps,"[33] not realizing the actual cost of their transaction. This system of unprotected health information commodification exacerbates the flaws in the segmented reality of consumer privacy. However, this concern has been a popular area of discussion, with recent developments in the FTC and several states. Colorado and Virginia have both recently passed state privacy laws, and other states have introduced bills to implement additional privacy laws, which will be forthcoming developments to monitor.[34] Given the numerous and continuous changes in privacy laws, this article will not be comprehensive, but rather, focus on developments in the FTC's Breach Notification Rule amended in September 2021, California's forthcoming 2022 privacy amendments, and conclude by examining Illinois' Biometric Information Privacy Act, which has recently seen a large increase of claims.

II. THE FTC'S NEW CLASSIFICATION OF DEVELOPERS AS "HEALTH CARE PROVIDERS"

On September 15, 2021, the FTC issued its Policy Statement for the FTC's Health Breach Notification Rule (the "Rule"), explaining that a "developer of a health app or connected device is a 'health care provider' because it furnish[es] health care services or supplies."[35] FTC Chair Lina M. Khan explained that "while this Rule imposes

---

[30] Rebecca Lipman, *Online Privacy and the Invisible Market for Our Data*, 120 DICK. L. REV. 780, 777-806 (2016).

[31] Clayton et al., *supra* note 17, at 35.

[32] Rosas, *supra* note 13, at 335.

[33] Lipman, *supra* note 30.

[34] *U.S. State Privacy Legislation Tracker*, INT'L ASS'N PRIVACY PROF. (Sept. 2021), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ (last visited Dec. 21, 2021).

[35] *Statement of the Commission*, *supra* note 2.

some measure of accountability on tech firms that abuse our personal information, a more fundamental problem is the commodification of sensitive health information, where companies can use this data to feed behavioral ads or power user analytics."[36] This change allows for non-HIPAA covered entities "to face accountability when consumers' sensitive health information is breached."[37]

Under the Rule, "vendors of personal health records ("PHR") and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information or face civil penalties for violations. The Rule also covers service providers to these entities."[38] This classification of developers as health care providers has serious implications for developers because it covers anyone creating apps that collect health information, even tangentially.[39] The FTC intends to enforce the Rule "with vigor"[40] with this new classification and with penalties of $43,792 per violation per day.[41] Enforcement of the Rule may prove to be largely effective given the federal nature of the Rule, rather than requiring compliance with separate state breach notification laws, which poses many challenges.[42]

Although they are not perfect,[43] breach notifications provide several benefits to consumers, such as notice and knowledge in order to file a complaint and allow consumers to take action once their

---

[36] *FTC Warns Health Apps and Connected Device Companies to Comply With Health Breach Notification Rule*, FED. TRADE COMM'N (Sept. 15, 2021), https://www.ftc.gov/news-events/press-releases/2021/09/ftc-warns-health-apps-connected-device-companies-comply-health.

[37] *Id.*

[38] *Id.*

[39] *Id.*

[40] *Remarks by Chair Lina M. Khan on the Health Breach Notification Rule Policy Statement Commission File No. P205405*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/documents/public_statements/1596360/remarks_of_chair_lina_m_khan_regarding_health_breach_notification_rule_policy_statement.pdf (last visited Dec. 20, 2021).

[41] *Statement of the Commission*, *supra* note 2.

[42] Charlotte Tschider, *Experimenting with Privacy*, 18 TUL. J. TECH. & INTELL. PROP. 45, 49 (2015) (explaining that state "laws have resulted in fragmented data protection, a particular lack of consistency for interstate commerce, differing requirements for multifunctional corporations, and challenging interpretations for foreign corporations adequately protecting consumer data.").

[43] Rachel M. Peters, *So You've Been Notified, Now What: The Problem with Current Data-Breach Notification Laws*, 56 ARIZ. L. REV. 1171 (2014) (explaining that even if notification is effective, consumers may be left with little recourse).

information has been compromised,[44] incentives for entities to protect data,[45] and the possibility to reduce the occurrence of identity theft.[46] State breach notification laws and HIPAA's Breach Notification Rule require notice to affected individuals notice once there has been a breach of their information.[47] Although the Rule similarly requires notification to the Commission itself of such a breach, previously, the FTC merely issued best practices guidelines for developers.[48] The Commission has never enforced the Rule prior to this Policy Statement.[49]

III. FTC ACTION PRIOR TO THIS UPDATE

In January 2021, prior to this extension of the Rule, Flo Health Inc., a fertility tracking application, settled against FTC allegations of sharing millions of users' sensitive health data with marketing firms, analytics firms, Facebook, and Google after promising to keep such information private.[50] The complaint alleged that the app, which was used by over 100 million consumers, disclosed sensitive health information as "app events" that were shared with third parties.[51] The complaint alleged misrepresentations regarding privacy, notice, choice, accountability for onward transfers [of data], and integrity and purpose limitation in violation of Section 5(a) of the FTC Act.[52] Although the

---

[44] Sara A. Needles, *The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law*, 88 N.C. L. REV. 267, 272 (2009).

[45] Richard J. Sullivan & Jesse Leigh Maniff, *Data Breach Notification Laws*, FED. RSRV. BANK KAN. CITY, https://www.kansascityfed.org/documents/336/2016-Data%20Breach%20Notification%20Laws.pdf (last visited Dec. 20, 2021).

[46] *Id.*

[47] *Breach Notification Rule*, HEALTH & HUM. SERV. (July 2013), https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (last visited Dec. 20, 2021).

[48] Mobile Health App Developers: FTC Best Practices, FED. TRADE COMM'N (Apr. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-app-developers-ftc-best-practices (last visited Dec. 20, 2021).

[49] *Statement of the Commission*, *supra* note 2.

[50] *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, FED. TRADE COMM'N (June 2021), https://www.ftc.gov/news-events/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared (last visited Dec. 20, 2021).

[51] *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that it Misled Consumers About the Disclosure of their Health Data*, FED. TRADE COMM'N (Jan. 2021), https://www.ftc.gov/news-events/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc (last visited Dec. 20, 2021).

[52] Complaint, *in the Matter of Flo Health Inc.*, No 1923133 (FTC June 22, 2021).

updated Rule did not apply in this case, the settlement required Flo Health to notify affected users about the disclosure and to instruct third parties to destroy such data.[53] Flo Health was also prohibited from misrepresenting the purpose of data collection, maintenance, use, and disclosure, how consumers can control data uses, and other similar misrepresentations.[54] The FTC further issued guidance to consumers regarding health apps,[55] and subsequently extended the Rule's scope. Prior to amending the Rule, the FTC, along with its authority to enforce consumer privacy with Section 5(a) of the FTC Act, also has had authority to enforce data security.[56]

Expansion of the Rule will allow for timely enforcement, as health apps, especially "software, diagnostics, products, and services that use technology to focus on women's health," called "Femtech," is on the rise.[57] Femtech focuses on "fertility solutions, period-tracking, pregnancy and nursing care, women's sexual wellness, and reproductive system health care" and in 2015, 82 million dollars were invested into nine Femtech companies.[58] The problem with Femtech, like Flo Health, is that it often prompts users to insert their "health history for more accurate analytics," which may include information that may be in medical records such that "the application monitors a user's health status to the same extent a physician or gynecologist would," rendering this previously protected information unprotected.[59]

IV. CALIFORNIA

Recent California privacy discussions have focused on the California Consumer Privacy Act of 2018 ("CCPA")[60] and the California Privacy Rights Act of 2020 ("CPRA").[61] The CCPA excludes certain personal information covered through other means, such as HIPAA,

---

[53] *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, *supra* note 50.

[54] *Id.*

[55] *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that it Misled Consumers About the Disclosure of their Health Data*, *supra* note 51.

[56] Lipman, *supra* note 30, at 790 (explaining that *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015) confirmed the FTC's authority over data security).

[57] Rosas, *supra* note 13, at 320.

[58] *Id.*

[59] *Id.* at 329.

[60] CAL. CIV. § 1798.100 (West).

[61] Letter from Alastair Mactaggart, Bd. Chair Cal. for Consumer Priv., to Initiative Coordinator for the Attorney General's Office (Nov. 13, 2019) (available at https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf).

but indeed protects other health information under the broad definition of "personal information" in the statute.[62] However, there are two additional developments relating to personal health information privacy in California, specifically, pertaining to genetic information.

First is an amendment to add "genetic information" in the definition of "personal information" in California's breach notification law (Cal. Civ. Code Section 1798.29 & 1798.82) and California's data security law (Cal. Civ. Code Section 1798.81.5), which require notification in the event of a breach.[63] Although both laws already include medical, health insurance, and biometric information in their definitions of personal information,[64] this addition of genetic information will expand the definition of personal information to include "any data, regardless of its format, that results from the analysis of a biological sample of an individual, or other source, and concerns genetic material, as specified."[65]

The second is a new law focused on DTC-GT companies' collection of genetic information. On January 1, 2022, California's Genetic Information Privacy Act will come into effect.[66] This will require DTC-GT companies "to provide a consumer with certain information regarding the company's policies and procedures for the collection, use, maintenance, and disclosure, as applicable, of genetic data, and to obtain a consumer's express consent for collection, use, or disclosure of the consumer's genetic data, as specified."[67]

California state law regulating DTC-GT companies' data collection is significant because at a federal level, DTC-GT is not assessed through the Food and Drug Administration ("FDA") review and approval process that is required in drug development, but rather, is evaluated through a less stringent approval method as a medical device,[68] and therefore, is regulated through the Food, Drug, and Cosmetic Act.[69] In the consumer law space, issues exist regarding the accuracy and representations of DTC-GT companies and their services,[70] as well

---

[62] CIV. § 1789.100.

[63] *California Enacts New Privacy Law for Genetic Data*, THE NAT'L LAW REV. (Oct. 12, 2021), https://www.natlawreview.com/article/california-enacts-new-privacy-law-genetic-data (last visited Dec. 20, 2021).

[64] CAL. CIV. §§ 1798.29, 1798.82 & 1798.81.5 (West).

[65] *California Enacts New Privacy Law for Genetic Data*, *supra* note 63.

[66] *Id.*

[67] *Id.*

[68] *Products and Medical Procedures*, FOOD & DRUG ADMIN. (Sept. 2021), https://www.fda.gov/medical-devices/products-and-medical-procedures (last visited Dec. 21, 2021).

[69] Gniady, *supra* note 18, at 2437.

[70] *Id.* at 2446.

as concerns regarding privacy.[71] In 2017, the FDA granted approval to certain 23andMe tests citing a user study that found that 23andMe's "instructions and reports were easy to follow and understand" and that consumers "understood more than ninety percent of the information presented in the reports."[72] However, this understanding pertains to the genetic reports themselves, not the terms and conditions or privacy policies of such tests. Privacy concerns include not only a consumer's individual genetic information, but also that of their relatives.[73] In assessing privacy policies of DTC-GT companies, a number of policies explain that they can sell or share information with third parties, while some policies omit this information entirely.[74] Such DTC-GT policies often include a "business transfer clause" which allow for transferability of a company's assets, which include consumers' DNA, in the event of a sale, acquisition or merger, meaning that there is nothing stopping 23andMe from selling information to Facebook, for example.[75] Selling, sharing, and transferring of data is not merely a possibility, as in 2018, 23andMe announced it would share more than five million consumers' genetic information with "GlaxoSmithKline to translate genetic and phenotypic data into targeted pharmaceutical treatments."[76] Time will tell if California's express consent requirement for use and disclosure of consumer genetic information will be an effective method to protect consumers in these scenarios.

As of 2020, about thirty million consumers have used DTC-GTs.[77] Large amounts of data, coupled with a lack of regulation pose serious risks for unauthorized exposure of consumer information, even if it is not genetic information.[78] In 2017, MyHeritage, a DTC-GT

---

[71] Clayton et al., *supra* note 17, at 2.

[72] *FDA Allows Marketing of First Direct-to-Consumer Tests That Provide Genetic Risk Information for Certain Conditions*, FOOD & DRUG ADMIN. (Apr. 2017), https://www.fda.gov/news-events/press-announcements/fda-allows-marketing-first-direct-consumer-tests-provide-genetic-risk-information-certain-conditions (last visited Dec. 21, 2021).

[73] Alyssa K. McLeod, *Sales, Acquisitions, and Mergers of Direct-to-Consumer Genetic Testing Companies: The Risks and a Solution*, 8 TEX. A&M L. REV. 405, 403-421 (2021).

[74] *Id.* at 406.

[75] *Id.* at 410.

[76] Rachele M. Hendricks-Sturrup, et al., *Direct-to-Consumer Genetic Testing and Potential Loopholes in Protecting Consumer Privacy and Nondiscrimination*, 321, JAMA 1869, 1870 (2019).

[77] Victoria Romine, *Crime, DNA, and Family: Protecting Genetic Privacy in the World of 23andMe*, 53 ARIZ. ST. L.J. 367, 373 (2021).

[78] Juan Pablo Sarmiento Rojas, *Direct-to-Consumer Genetic Testing: Rethinking Privacy Laws in the United States*, 14 HEALTH L. & POL'Y BRIEF 21, 33 (2020).

company, suffered a breach that compromised over ninety-two million consumers' accounts.[79] Although this breach did not compromise genetic data, it exposed consumers' email and password information.[80] Under current federal laws, MyHeritage would not have been liable for failing to protect this information, even if there had been genetic information in the breach.[81] Given the nature of genetic information, a breach would not only impact the consumer who used the DTC-GT, but also their blood relatives.

This recognition of the importance of genetic information in California is opportune, as experts are concerned about the increased use of readily available genetic information. For example, in 2018 California's "Golden State Killer" was caught after an online database linked him with users who had DNA equivalent to third cousins to him.[82] DTC-GT companies hold so much data, that the average consumer who uses a DTC-GT company has "nearly 200 third cousins, 950 fourth cousins, and 4,700 fifth cousins."[83] Consumers thus have the ability to match with relatives stemming back to thousands of years ago, with this collection of information only growing.[84] Given that genetic privacy goes beyond the individual, this becomes a privacy issue for law enforcement as well. Law enforcement uses the National DNA Index ("NDIS"), which contains almost two million samples of DNA from criminal investigations and criminal defendants, as well as the Combined DNA System Index System ("CODIS"),[85] which when used in conjunction with genetic information from DTC-GTs online, creates a larger threat to privacy because "none of the available DTC databases allow a user's genetic relatives to 'opt out' of law-enforcement access."[86]

There are possible genetic data privacy-preserving solutions that DTC-GT companies could implement to protect the security of their data, such as cryptographic primitives, which are "algorithms used to build cryptographic systems to provide information security"[87]

---

[79] *Id.* at 33-34.
[80] *Id.* at 34.
[81] *Id.*
[82] Jocelyn Kaiser, *We Will Find You: DNA Search Used to Nab Golden State Killer Can Mome in on About 60% of White Americans*, SCIENCE (Oct. 2018), https://www.science.org/content/article/we-will-find-you-dna-search-used-nab-golden-state-killer-can-home-about-60-white (last visited Dec. 20, 2021).
[83] Romine, *supra* note 77.
[84] *Id.*
[85] *Id.* at 373-375.
[86] *Id.* at 379.
[87] Yakubu & Chen, *supra* note 22, at 517.

as well as several system architecture framework types and models used to protect genomic data.[88] But, these security measures are not foolproof solutions, as these are not applicable in non-breach or non-genomic privacy attack situations, such as a DTC-GT company willingly sharing or selling its information. So, even the most secure data could still threaten consumers' privacy through a DTC-GT company's privacy policy permitting selling and sharing of data. Overall, the use of genetic information is a complex issue with Fourth Amendment implications[89] beyond the scope of this paper, and experts will likely continue to discuss potential effects of DTC-GTs on privacy, such as the erosion of public trust and discrimination.[90]

V. ILLINOIS

Illinois is a leader in protecting biometric data, as evidenced by the Illinois Biometric Information Privacy Act ("BIPA"), which regulates "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information" and allows for a private right of action.[91] Like the FTC's Breach Notification Rule, BIPA was enacted over a decade ago, but recently has seen an increase of claims.[92] BIPA requires that before the collection of biometric information, a private entity "must inform the individual that a biometric identifier, or biometric information, is being collected and inform them of the purpose and length of the collection and storage of their biometric information;" such "disclosures must be in writing, and the individual must provide a written release."[93]

Biometric information under BIPA includes "biometric identifiers" and "biometric information."[94] Biometric identifiers are defined as "a retina or iris scan, fingerprint, voiceprint, or a scan of hand or face geometry but excludes certain personal information from the definition of biometric identifier, such as handwriting samples, tattoos,

---

[88] *Id.* at 512.

[89] Romine, *supra* note 77, at 385-388 (discussing *Carpenter v. United States*, where a reasonable expectation of privacy was not revoked by the third-party doctrine).

[90] Hendricks-Sturrup et al., *supra* note 76, at 1869.

[91] Biometric Information Privacy Act, 740 ILL. COMP. STAT. ANN. 14 (2008).

[92] Rachel Nevarez & Michael Barnes, *Litigants Continue to Test Bounds of Illinois' Biometric Information Privacy Act Following Illinois Supreme Court's Finding That a Plaintiff Need not Have an Actual Injury to Recover Damages*, DUPAGE CNTY. BAR ASSN., https://www.dcba.org/mpage/v33-Nevarez-Barnes (last visited Dec. 20, 2021).

[93] Charles N. Insler, *Understanding the Biometric Information Privacy Act Litigation Explosion*, 106 ILL. B.J. 34, 35 (2018).

[94] Nevarez & Barnes, *supra* note 92.

physical descriptions, and photographs."[95] Biometric information includes "any information," regardless of how it is captured, converted, stored, or shared that is based upon a biometric identifier" and excludes "information captured from a patient for medical treatment and certain information collected under various other statutes."[96] Notably, BIPA does not require actual injury, rather, the Illinois Supreme Court clarified that there merely needs to be a technical violation.[97]

In 2015, Facebook users alleged that the company's "Tag Suggestions" program, which "searches for and identifies people's faces in photographs uploaded to Facebook to promote user tagging," violated BIPA.[98] Facebook's settlement payment was $650 million, and the company agreed to use an affirmative, opt-in consent model for its biometric uses, among other changes.[99] The final order recognized that this settlement was "a major win for consumers in the hotly contested area of digital privacy."[100]

In 2019, a vending machine user sued Compass Group, the nation's largest vending machine services company, and 365 Retail Markets, a global technology provider for vending machines, claiming that their Smart Market vending machine used her fingerprint without notice.[101] The vending machines "did not accept cash; instead, a user had to establish an account using her fingerprint," which is considered a biometric identifier under BIPA.[102] The plaintiff claimed that "Compass's failure to make the requisite disclosures denied her the ability to give informed written consent as required" by BIPA and that this failure resulted in "the loss of the right to control their biometric identifiers and information."[103] On appeal, the Court of Appeals for the Seventh Circuit explained that "the statute demonstrates that its purpose is to ensure that consumers understand, before providing their biometric

---

[95] *Id.*

[96] *Id.*

[97] *Id.*

[98] Order, *In re Facebook Biometric Information Privacy Litigation*, U.S. District Court Northern District of CA, Feb. 26, 2021. https://cdn.vox-cdn.com/uploads/chorus_asset/file/22333300/In_re_Facebook_Biometric_Information_Privacy_Litigation_final_order.pdf

[99] *Id.*

[100] *Id.*

[101] Pl.'s Mem. of Laws in Supp. of her Unopposed Mot. for Prelim. Approval of Class Action Settlement, *Christine Bryant vs. Compass Group USA Inc. and 365 Retail Markets, LLC*, Oct. 28, 2021. https://fingfx.thomsonreuters.com/gfx/legaldocs/lgpdwlymnvo/Compass%20Preliminary%20Approval%20Memo.pdf

[102] Bryant v. Compass Group USA, Inc., 958 F.3d 617, 619 (7th Cir. 2020).

[103] *Id.* at 623.

data, how that information will be used, who will have access to it, and for how long it will be retained" and that the omission of terms were not merely a "failure to satisfy a purely procedural requirement," but rather, an injury-in-fact.[104] In the proposed class action settlement filed on October 28, 2021, both companies agreed to pay $6.8 million to resolve the claims.[105] Illinois has seen numerous BIPA claims in the past few years, spanning across various areas of law, including labor and employment, health law, and commercial law with new products that rely on biometrics. As an example, another recent BIPA claim was settled when Corner Bakery Café settled a class action claim that its biometric clock system used to record employees' time worked violated BIPA because they did not obtain employees' prior written consent of such use of their biometric information.[106] The Corner Bakery Café settled in October 2020 for $3,242,400.[107]

VI. CONCLUSION

The increased quantity of unprotected health information in the IoMT and held by DTC-GT companies, coupled with big data capabilities and a lack of consumer knowledge, creates various vulnerabilities for consumers. On the other hand, these technological advances also pose great benefits for consumers as they have potential to improve statistical tools and learning algorithms, reduce costs, improve healthcare outcomes, and produce system-wide innovations, among other benefits.[108] These new developments in the FTC and California, and an increase of BIPA actions in Illinois show the need for additional safeguards to parallel the increase of health information in the IoMT to improve consumer rights and protections.

---

[104] *Id.* at 626.
[105] Order, *supra* note 98.
[106] Final Approval Order, *Jones v. CBC Restaurant Corp*, 2020 WL 8673114 (Verdict, Agreement and Settlement)
United States District Court, N.D. Illinois, Eastern Division.
[107] *Id.*
[108] Yuan, *supra* note 6, at 6.