HEALTH DATA AT YOUR FINGERTIPS: FEDERAL REGULATORY PROPOSALS FOR CONSUMER-GENERATED MOBILE HEALTH DATA

Jianyan Fang*

CITE AS: 4 GEO. L. TECH. REV. 125 (2019)

TABLE OF CONTENTS

* LL.M. graduate, Harvard Law School. I am grateful to Professor I. Glenn Cohen, who supervised this article's preparation and offered insightful comments. I also benefitted from the helpful discussions with Professor Jonathan Zittrain and Professor William W. Fisher and the valuable comments from Jane Fair Bestor, Oren Tamir, and editors of this journal. Finally, I appreciate the research support provided by the staff of the Harvard Law School Library, especially Jennifer Allison.

"DATA IS THE NEW OIL."[1]

"HEALTH DATA IS VALUABLE: YOUR EMPLOYER WANTS IT, YOUR INSURERS WANT IT, AND YOU'RE ONLY TOO HAPPY TO GIVE IT AWAY TO APPS FOR FREE."[2]

I. INTRODUCTION

Are you male or female? When were you born? How tall are you? How much do you weigh? You may have encountered these questions when signing up with a fitness mobile application (app) like MyFitnessPal.[3] After you quickly provide this personal information, and consent to the app's privacy terms and cross-border data transfer policy, the app would be able to track, store, and analyze your diet, steps, exercise, and other daily activities to help you lose weight and promote a healthy lifestyle.

When you search terms such as "health," "fitness," "wellness," and "diagnosis" in the App Store or Google Play Store, hundreds of apps like MyFitnessPal will pop up—all making promises of better health. These apps target a variety of users such as consumers, doctors, and medical students.

Statistics show that around 318,000 mobile health (mHealth) apps are now available in major app stores, and the global mHealth app market is

[1] Nicolas P. Terry, *Will the Internet of Things Transform Healthcare*, 19 VAND. J. ENT. & TECH. L. 327, 337 (2016).
[2] Angela Lashbrook, *There Is a Reason Apps Make It So Fun to Track Your Health the Outline*, THE FUTURE (Feb. 1, 2019, 1:30 PM), https://theoutline.com/post/7039/there-is-a-reason-apps-make-it-so-fun-to-track-your-health [https://perma.cc/FB4W-GHAM].
[3] MYFITNESSPAL, https://www.myfitnesspal.com/ [https://perma.cc/QEV3-E56D].

expected to reach 111 billion U.S. dollars by 2025.[4] Half a billion smartphone users have installed at least one mHealth app on their phones.[5] Continuous market growth and widespread use of these apps have made mHealth an important segment of the health industry and part of our daily lives. mHealth technologies are allowing the devices we take everywhere to constantly collect and share our health data.

Many believe mHealth has the potential to strengthen the "iron triangle of health care" by enhancing quality, decreasing cost, and improving access.[6] However, these benefits are not without privacy risks. In November 2018, DeepMind Health, a London-based health app team focusing on artificial intelligence (AI) research and mobile tools,[7] announced that it was joining Google Health.[8] This news has caused wide concerns over DeepMind Health's independence from Google in dealing with health data.[9] Only weeks later, the French regulator fined Google nearly $57 million for failing to properly disclose its data collection across its various services in accordance with the European Union (EU) General Data Protection Regulation (GDPR),[10] suggesting that such concerns are not without basis. In the United States, Facebook was reported to have received health data from third-party health

[4] *11 Surprising Mobile Health Statistics*, MOBIUS MD, https://www.mobius.md/blog/2019/03/11-mobile-health-statistics/ [https://perma.cc/9GP6-CJKT].

[5] Dov Greenbaum, *Avoiding Overregulation in the Medical Internet of Things, in* BIG DATA, HEALTH LAW, AND BIOETHICS 129, 132 (I. Glenn Cohen et al. eds., 2018).

[6] Cheng-Kai Kao & David M. Liebovitz, *Consumer Mobile Health Apps: Current State, Barriers, and Future Directions*, 9 PHYSICAL MED & REHABILITATION 106, 106 (2017).

[7] Dominic King, *DeepMind's Health Team Joins Google Health*, DEEPMIND, (Sept.18, 2019), https://deepmind.com/blog/announcements/deepmind-health-joins-google-health [https://perma.cc/D4JA-TXRG].

[8] Demis Hassabis, Mustafa Suleyman & Dominic King, *Scaling Streams with Google*, DEEPMIND (Nov. 13, 2018), https://deepmind.com/blog/announcements/scaling-streams-google [https://perma.cc/4W7J-XL2P].

[9] Margi Murphy, *Privacy Concerns as Google Absorbs DeepMind's Health Division*, TELEGRAPH (Nov. 13, 2018, 10:40 PM), https://www.telegraph.co.uk/technology/2018/11/13/privacy-concerns-google-absorbs-deepminds-health-division/ [https://perma.cc/867Y-ZZ2P].

[10] Adam Satariano, *Google Is Fined $57 Million Under Europe's Data Privacy Law*, N.Y. TIMES (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html [https://perma.cc/GS5T-WVAA].

and fitness apps, potentially without notifications to users;[11] the data transmitted included diet information, exercise activities, ovulation cycle, and intention to get pregnant.[12] Five months later, Facebook was fined $5 billion by the Federal Trade Commission (FTC) based on its repeated breaches of its previous 2011 privacy protection settlement with the regulator.[13]

Unlike the EU and many other peer countries such as Canada, Israel, and Japan,[14] the United States is not keen on comprehensive protection of personal data. In the absence of an overarching data protection framework, the United States sticks with a "sectoral" privacy regulatory system[15] where only certain sensitive, high-stakes sectors receive exceptional statutory privacy protection. In terms of general privacy concerns, the United States relies on the competent regulator's case-by-case, light-touch enforcement actions from the perspective of consumer protection.[16]

Unsurprisingly, healthcare has been singled out as one of the sectors receiving exceptional privacy protection. Health data is traditionally protected by the Health Insurance Portability and Accountability Act (HIPAA), which is enforced by the U.S. Department of Health and Human Services (HHS).[17]

---

[11] Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook.*, WALL ST. J. (Feb. 22, 2019, 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636 [https://perma.cc/GC8T-8UHC]; *see also* Nick Statt, *App Makers Are Sharing Sensitive Personal Information with Facebook but Not Telling Users*, VERGE (Feb. 22, 2019, 2:00 PM), https://www.theverge.com/2019/2/22/18236398/facebook-mobile-apps-data-sharing-ads-health-fitness-privacy-violation [https://perma.cc/R6QW-MXDR].

[12] *Id.*

[13] Levi Sumagaysay, *Facebook Settlement Confirmed: Are $5 Billion Fine and Limits on Zuckerberg Enough?*, MERCURY NEWS (July 24, 2019, 3:34 PM), https://www.mercurynews.com/2019/07/24/facebook-settlement-confirmed-are-5-billion-fine-and-limits-on-zuckerberg-enough/ [https://perma.cc/DPS7-WD85].

[14] Nuala O'Connor, *Reforming the U.S. Approach to Data Protection and Privacy*, COUNCIL ON FOREIGN REL. (Jan. 30, 2018), https://www.cfr.org/report/reforming-us-approach-data-protection [https://perma.cc/EDN6-9TXC].

[15] Anne Marie Helm & Daniel Georgatos, *Privacy and MHealth: How Mobile Health Apps Fit into a Privacy Framework Not Limited to HIPAA*, 64 SYRACUSE L. REV. 131, 140 (2014).

[16] *See generally* Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of the FTC Data Protection*, 83 GEO. WASH. L. REV. 2230 (2015) (discussing the scope of FTC's authority in the area of data protection and its limits, arguing that FTC's current modest enforcement only focuses on the most egregious violations, and urging FTC to strengthen and improve its enforcement actions); Fed. Trade Comm'n, *A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority,* FTC.GOV (revised Oct. 2019) https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority (providing an overview of FTC's various enforcement powers including, among others, its consumer protection power under Section 5 of the FTC Act) [https://perma.cc/66SK-WJV6]; *see also* discussions *infra* Part III

[17] Margaret Foster Riley, *Big Data, HIPAA, and the Common Rule Time for Big Change?,* BIG DATA, HEALTH LAW, AND BIOETHICS 251, 260 (I. Glenn Cohen et al. eds., 2018).

However, mHealth has posed new challenges for HIPAA. Enacted in pre-mHealth times, HIPAA regulates health data only to the extent that it is disclosed and used by covered entities[18] and business associates[19] as defined under HIPAA.[20] As the collectors and custodians of HIPAA-regulated health data, most HIPAA-defined covered entities and business associates are traditional players within the healthcare sector; they typically include health plans, healthcare clearinghouses, healthcare providers and independent contractors acting on their behalf.[21] Because most consumer-facing mHealth apps are developed and used without the involvement of HIPAA-defined covered entities or business associates, health data collected and generated by these consumer grade apps usually falls outside the purview of HIPAA.[22]

In addition to HHS, FTC—as mentioned in the Facebook example above—and the Food and Drug Administration (FDA) are two of the primary federal regulators of the mHealth industry identified by the American Health Information Management Association.[23] Both FTC and FDA have intervened in this industry to varying degrees, but have failed to provide complete protection for mHealth app data. FTC's enforcement power is broad,[24] but the Commission must establish "deceptiveness"[25] or "unfairness"[26] before policing any breach of mHealth app data. FDA, whose focus is to supervise the efficacy of mHealth apps and protect public health,[27] is not concerned with protecting privacy.[28]

The development of the mHealth industry has outpaced the existing federal health data protection regime. To fill the regulatory gaps,

---

[18] 45 C.F.R. § 160.103 (2019).
[19] *Id.*
[20] 45 C.F.R. § 160.102 (2019); *see also* discussion *infra* Part III.A.
[21] 45 C.F.R. § 160.102 (2019).
[22] See Jessica Davis, *HHS Clarifies HIPAA Liability Around Third-Party Health Apps*, XTELLIGENT HEALTHCARE MEDIA, (Apr. 12, 2019), https://healthitsecurity.com/news/hhs-clarifies-hipaa-liability-around-third-party-health-apps [https://perma.cc/46QY-HJ84?type=image].
[23] Y. Tony Yang & Ross D. Silverman, *Mobile Health Applications: The Patchwork of Legal and Liability Issues Suggests Strategies to Improve Oversight*, 33 HEALTH AFF. 222, 223 (2014) (noting that in addition to HHS, the FTC, and the FDA, the National Institute of Standards and Technology and the Federal Communications Commission are also likely to be involved in regulating mHealth apps).
[24] Hartzog & Solove, *supra* note 16, at 2246.
[25] 15 U.S.C. § 45(a)(1).
[26] *Id.*
[27] Matthew R. Langley, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 GEO. L.J. 1641, 1650 (2015).
[28] FUTURE PRIVACY FORUM, BEST PRACTICES FOR CONSUMER WEARABLES & WELLNESS APPS & DEVICES, 1 n.2 (2016), https://fpf.org/wp-content/uploads/2016/08/FPF-Best-Practices-for-Wearables-and-Wellness-Apps-and-Devices-Final.pdf [https://perma.cc/R3S6-HJ8U].

commentators have made various recommendations. Many have proposed expanding and updating HIPAA to include and accommodate "non-HIPAA" health data.[29] Some have suggested passing a specific, standalone statute to protect non-HIPAA health data.[30] Others have considered self-regulation and

[29] *See generally* Alexis Guadarrama, *Mind the Gap: Addressing Gaps in HIPAA Coverage in the Mobile Health Apps Industry*, 55 HOUS. L. REV. 999 (2018) (discussing the gap of HIPAA coverage in regulating mobile health apps and suggesting expanding HIPAA to cover private heath data regardless of who holds it); Latena Hazard, *Is Your Health Data Really Private: The Need to Update HIPAA Regulations to Incorporate Third-Party and Non-Covered Entities*, 25 CATH. U. J. L. & TECH 447 (2017) (discussing, among others, HIPAA rules and their effect on health apps, and arguing that HIPAA needs to be adjusted to incorporate non-covered entities); Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143 (2017); Grant Arnow, *Apple Watching You: Why Wearable Technology Should Be Federally Regulated*, 49 LOY. L.A. L. REV. 607 (2016) (proposing establishment of a standalone, cabinet-level department to align and unify national Internet data protection efforts and suggesting updating HIPAA); Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16 YALE J. HEALTH POL'Y L. & ETHICS 1 (2016) (discussing the growth of employee-facing health and fitness apps and increased employee monitoring, examining the current data protection regulations and agency actions, and proposing the adoption of a mandatory privacy labeling law for health-related devices and apps, and suggesting expanding HIPAA's protection); Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65 (2014); Nicolas Terry, *Health Privacy is Difficult But Not Impossible in a Post-HIPAA Data-driven World*, 146 CHEST 835 (2014) (taking the position that health-care-data exceptionalism remains a valid policy and the current HIPAA protection model should be maintained and re-calibrated to consider the upstream and point-of-use protections and protect healthcare data residing outside of the traditional health-care domain).

[30] *See generally* Michelle M. Christovich, *Why Should We Care What Fitbit Shares—A Proposed Statutory Solution to Protect Sensitive Personal Fitness Information*, 38 HASTINGS COMM. & ENT. L.J. 91 (2016) (suggesting, among others, that Congress should adopt a statutory scheme modeled after HIPAA to adequately protect users' privacy rights against the misuse of fitness information).

co-regulation approaches for protection of mHealth app data, or more generally, consumer privacy.[31]

This Article joins these discussions to explore how mHealth app data can be better protected on the federal level. It aims to contribute to the academic literature in two ways. First, it engages in a detailed rethinking of the concept of health data and frames a two-step approach to define health data in the era of Big Data. Second, unlike those scholarly discussions proposing one-size-fits-all solutions, this Article envisions a single two-prong solution to accord different levels of protection to different categories of mHealth app data and to balance the necessity of privacy protection with commercial needs. The first prong is to expand HIPAA to cover high-stakes mHealth app data that qualifies as health data warranting extra protection under the new definition proposed by this Article. The second prong is to adopt a co-regulation approach to govern the less sensitive mHealth app data that does not fall under the proposed new definition of health data.

This Article focuses exclusively on federal-level regulations; state-level regulatory solutions are therefore not reviewed. Furthermore, this Article treats protection of mHealth app data as a consumer privacy issue and will discuss this issue only from the perspective of the private sector. It will not consider the regulation of the U.S. government's collection and use of health data.

The remainder of this Article proceeds as follows: Part II portrays the current state of mHealth apps and mHealth app data and proposes a two-step approach to define health data in the era of Big Data. Part III assesses the current U.S. federal regulatory system of health data and identifies the regulatory gaps for protection of mHealth app data. Part IV argues that regulation is necessary for mHealth app data, and that the government needs

---

[31] *See generally* Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461 (2016) (discussing the key role of collaborative governance in creating a regulatory framework that both protects consumers and the businesses); J. Frazee, M. Finley & J.J. Rohack, *mHealth and Unregulated Data: Is This Farewell to Patient Privacy*, 13 IND. HEALTH L. REV. 384 (2016) (proposing a voluntary labelling system and arguing that allowing voluntary adoption of the labelling system rather than mandating increased privacy protections would allow companies to provide free options to consumers while providing privacy conscious consumers with a meaningful choice); Dennis D. Hirsch, *Going Dutch: Collaborative Dutch Privacy Regulation and the Lessons It Holds for U.S. Privacy Law*, 2013 MICH. ST. L. REV. 83 (2013) (introducing the Dutch code of conduct approach, and discussing the lessons the US can draw from the Dutch experience in maximizing strengths and minimizing weaknesses of the code of conduct approach); Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 ISJLP 355 (2011) (discussing different types of self-regulation and exploring co-regulatory approaches in which government sets requirements and imposes sanctions for non-compliance for the purpose of protecting online privacy).

to play a role in such regulation. The final part of this Article discusses in detail the proposed two-prong solution for regulating mHealth app data.

II. BIG HEALTH DATA, BIG CONCERNS, AND MHEALTH APP DATA

A. Categories of mHealth Apps and Working Definitions

In general, any medical and public health practice supported by mobile communication devices such as smartphones, tablets, wearable technology, and other wireless devices falls under the definition of "mobile health" or "mHealth."[32] mHealth apps can be downloaded and installed on mobile devices to perform designated medical or health-related functions.[33]

Scholars have developed various typologies for mHealth apps, most of which are functionality-based.[34] As one example, Nathan Cortez, a leading figure in the regulation of mobile health technologies and FDA regulation, divides mHealth apps into the following categories based on their respective functions: (1) connectors which connect mobile devices to FDA-regulated devices and thus amplify such regulated devices' functionalities; (2) replicators which turn mobile devices into FDA-regulated devices; (3) automators and customizers which use different methodologies including questionnaires, algorithms, formulae and medical calculators to aid clinical decisions; (4) informers and educators which primarily inform and educate users; (5) administrators which automate office functions such as identifying insurance billing codes or scheduling patient appointments; and (6) loggers and trackers which allow users to log, record, and make decisions about general health and wellness.[35]

---

[32] WORLD HEALTH ORG., MHEALTH: NEW HORIZONS FOR HEALTH THROUGH MOBILE TECHNOLOGIES, 6 (2011), https://www.who.int/goe/publications/goe_mhealth_web.pdf [https://perma.cc/6MBA-9TT7]; *see also* Nathan Cortez, *The Mobile Health Revolution*, 47 U.C. DAVIS L. REV. 1173, 1176 (2014) (defining "mobile health" as "the use of mobile communications devices like smartphones and tablet computers for health or medical purposes, usually for diagnosis, treatment, or simply well-being and maintenance"); Anne Marie Helm & Daniel Georgatos, *Privacy and MHealth: How Mobile Health Apps Fit into a Privacy Framework Not Limited to HIPAA*, 64 SYRACUSE L. REV. 131, 134 (2014) (noting that "mHealth occurs when a provider of healthcare services uses connected and interactive mobile computing to produce, access, transmit, or store data for the provision of healthcare services to patients, or when a patient or consumer uses connected and interactive mobile computing to produce, access, transmit, store, or otherwise share data for a health-related purpose").

[33] Guadarrama, *supra* note 29, at 1002.

[34] *See e.g.*, Nicholas P. Terry & Lindsay F. Wiley, *Liability for Mobile Health and Wearable Technologies*, 25 ANNALS HEALTH L. 62, 68 (2016); Cortez, *supra* note 32, at 1176.

[35] *Id.* at 1182–89.

In regulating the efficacy of mHealth apps, FDA has also adopted a similar functionality-based typology, but with more of a focus on risk control.[36] In its Policy for Device Software Functions and Mobile Medical Applications, FDA divides mHealth apps into three tiers. [37] The top tier represents "mobile medical apps" that operate as extensions of FDA-regulated medical devices, turn mobile platforms[38] into FDA-regulated devices, or function like FDA-regulated medical devices for analysis, diagnosis, and treatment purposes.[39] They qualify as "devices" defined under Section 201(h) of the Federal Food, Drug, and Cosmetic Act (FDCA),[40] and would pose a risk to a patient's safety if they do not function as intended.[41] The middle tier represents those mobile apps that *may* meet the definition of devices under the FDCA, but are not regulated as mobile medical apps because of their low risks.[42] The bottom tier represents mHealth apps that are not medical devices and therefore are not administered by FDA.[43] FDA claims that it intends (1) to apply oversight to the top tier of mHealth apps, (2) to exercise enforcement discretion (meaning it will not impose FDCA requirements)[44] over the middle tier, and (3) not to regulate the bottom tier.[45]

Some mHealth apps are consumer-facing, some require expertise, and many do not differentiate amongst target users at all.[46] Such user-based differentiation is meaningful for the purpose of this Article, and from a regulatory perspective as well. Because professional-facing mHealth apps are usually used or prescribed by HIPAA-regulated entities, such as healthcare

---

[36] *See generally* U.S. FOOD & DRUG ADMIN., POLICY FOR DEVICE SOFTWARE FUNCTIONS AND MOBILE MEDICAL APPLICATIONS GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2019), https://www.fda.gov/media/80958/download (providing detailed explanations in classifying mobile apps based on their potential risks posed to public health) [https://perma.cc/2WRD-5RHB].

[37] *See generally id.*

[38] *Id.* at 4 (Mobile platforms include smart phones, tablet computers, or other portable computers.).

[39] *Id.* at 11–12.

[40] 21 U.S.C. § 321(h) (2018) (defining a "device" in relevant part as: "an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is. . .intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or intended to affect the structure or any function of the body of man or other animals").

[41] U.S. FOOD & DRUG ADMIN., *supra* note 36, at 2.

[42] *Id.* at 9.

[43] *Id.* at 16.

[44] *Id.* at 2.

[45] *Id.*

[46] Cortez, *supra* note 32, at 1177.

professionals,[47] and data collected and generated by these apps is generally within the reach of HIPAA, they are not a concern of this Article. In contrast, consumer-facing mHealth apps, which are at the heart of this Article, are usually developed and used by entities not governed by HIPAA. Data collected and generated by these mHealth apps is by and large in a regulation-free zone.

However, under the current regulatory framework, this classification is not absolutely binary because the applicable data protection rules may vary as data changes hands. For example, a patient's blood pressure stored in a hospital's Electronic Health Record (EHR) is initially regulated by HIPAA, but it may escape from HIPAA's regulation once the patient downloads and inputs the same information into a consumer-facing mHealth app. Conversely, a user's blood pressure collected by a health management mobile app is free from regulation by HIPAA initially, but it will end up in EHR and be governed by HIPAA if the app user later transmits the blood pressure results to his or her physician for diagnosis or treatment purposes. This convertible situation will be further discussed in Part II of this Article.

To facilitate the subsequent discussions, unless otherwise stated, the term "mHealth app" hereinafter refers to consumer-facing mHealth apps used by individual consumers without the direct involvement of conventional healthcare providers[48] or other HIPAA-defined covered entities and business associates. The term "mHealth app data" refers to data of any nature that is collected and generated by consumer-facing mHealth apps and is not subject to the governance of the current HIPAA.[49] According to the various functions of mHealth apps discussed earlier, mHealth app data typically includes three groups of data: (1) health-related data, including medical history, test results, and clinical data, that has inherent medical significance and is used to identify an app user's particular condition, (2) biometrics information and lifestyle data that are somewhat related to an app user's body or general health and wellness, and (3) data that is normally not health-related, such as an app user's geolocation, identity, contact list, payment records, and social or recreational information.

---

[47] Nicolas P. Terry & Tracy D. Gunter, *Regulating Mobile Mental Health Apps*, 36 BEHAV. SCI. L. 136, 139 (2018).

[48] Nicolas P. Terry, *Mobile Health: Assessing the Barriers*, 147 CHEST 1429, 1430 (2015).

[49] *But see* Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143, 182 (2017) (mentioning that although the majority of mHealth apps are operating in the HIPAA-free zone, some developers of apps or wearables are beginning to advertise HIPAA-compliance).

B. Context Matters: Defining Health Data in the Era of Big Data

Big Data has obscured the distinction between different categories of data,[50] and is making it difficult to define precisely what health data encompasses. This Section will first discuss the concerns and problems brought about by Big Data analytics, and then propose a new definition of health data in the era of Big Data.

There are different understandings of Big Data. Some stress the characteristics of the data at issue and refer to Big Data as "large volumes of high-velocity, complex, and variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information."[51] Others focus on effects of the application of Big Data technologies and define Big Data as "a confluence of factors, including the nearly ubiquitous collection of consumer data from a variety of sources, the plummeting cost of data storage, and powerful new capabilities to analyze data to draw connections and make inferences and predictions."[52] Despite the nuances, the key implication is that Big Data analytics can shift the context of data use and creates a world where the significance and sensitivity of a single set of data will vary with the changing context. As a result, mundane data that is not inherently health-related could reveal health-related correlations or conclusions if aggregated and analyzed with other datasets.

Powered by Big Data analytics, ordinary consumer data is now widely used in health-related contexts. For example, a high school girl's purchasing data with the department store Target has been used to predict that she was pregnant – even before her father found out;[53] a childless man who does online clothing shopping, spends a lot on cable TV, and drives a minivan is inferably overweight;[54] a woman who purchases plus-size clothing is considered at risk

---

[50] Tal Z. Zarsky, *Incompatible: GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1013 (2017).

[51] Riley, *supra* note 17, at 252.

[52] FED. TRADE COMM'N, BIG DATA A TOOL FOR INCLUSION OR EXCLUSION: UNDERSTANDING THE ISSUES 1 (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/6P3X-4PA3].

[53] Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012, 11:02 AM), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#4ee5d5286668 [https://perma.cc/XBD4-VLRK].

[54] FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 30 (2015).

of depression;[55] and people downsizing homes tend to incur higher healthcare costs.[56] The former FTC Chairwoman Edith Ramirez has termed these predictions and inferences "data determinism" saying:

> [Persons are judged] . . .not because of what they've done, or what they will do in the future, but because inferences or correlations drawn by algorithms suggest they may behave in ways that make them poor credit or insurance risks, unsuitable candidates for employment or admission to schools or other institutions, or unlikely to carry out certain functions.[57]

Directed by data determinism, consumer categories such as "Expectant Parent," "Diabetes Interest," and "Cholesterol Focus" are created based on various ordinary consumer data that would not have been medically meaningful but for Big Data analytics.[58] Insurance companies,[59] credit-card companies,[60] and pharmaceutical companies[61] all utilize Big Data analytics to predict costs, calibrate rates, evaluate risks, and optimize target advertising.

Health professionals also seem to accept this blurred divide between health data and other data. Recognizing that many non-health social determinants and indicators are outside of the medical system,[62] the Institute of Medicine (IOM) recommended several years ago that federal health information technology (IT) policymakers should add new social and

---

[55] Marshall Allen, *Health Insurers Are Vacuuming Up Details About You—And It Could Raise Your Rates*, PROPUBLICA (Jul. 17, 2018, 5:00 AM), https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates [https://perma.cc/82P9-EFJY].

[56] *Id.*

[57] Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 79 (2014), http://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1005&context=healthmatrix [https://perma.cc/ZQ8X-MGSH].

[58] FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 47 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/J7CP-P937].

[59] Kaiser Health News, *Health Insurers Are Vacuuming Up Consumer Data That Could Be Used to Raise Rates*, HEALTHLEADERS (Jul. 17, 2018), https://www.healthleadersmedia.com/finance/health-insurers-are-vacuuming-consumer-data-could-be-used-raise-rates [https://perma.cc/7YSG-Q92S].

[60] Jay Hancock, *Is Your Private Health Data Safe In Your Workplace Wellness Program?,* PBS NEWSHOUR (Sep. 30, 2015, 6:07 PM), https://www.pbs.org/newshour/health/many-workplace-wellness-programs-dont-follow-health-privacy-laws [https://perma.cc/D9C4-Q7D3].

[61] Guadarrama, *supra* note 29, at 1013.

[62] Frank Pasquale, *Redescribing Health Privacy: The Importance of Information Policy*, 14 HOUS. J. HEALTH L. & POL'Y 95, 126 (2014).

behavioral information as part of the EHR to improve clinical research and healthcare delivery.[63] The recommended determinants and indicators include individuals' financial resource strain, level of physical activity, level of stress, educational status,[64] dietary patterns, employment, sexual orientation, and even neighborhood and community compositional characteristics.[65] As an example, according to IOM, the geographic location where an individual lives or works has no health-related significance on its face, but it can become medically revealing for the purpose of individual healthcare delivery or public health policies when it interacts with other datasets such as air pollution, the availability of sidewalks, public transportation, and healthy food options.[66]

A question follows: If the distinction between health data and other data is fading, is it even possible to define health data in this evolving setting? This Article argues that it is still possible to define health data because this blurring or confluence is not absolute but rather context-specific.

As discussed above, in the era of Big Data, aside from data's inherent nature, the context in which data is used is also a factor determining whether it will be considered health data in a particular circumstance. Accordingly, this Section proposes a two-step approach for defining health data.

First, the data in question should always be considered health data if it is intrinsically of medical significance, regardless of its sources, contexts for use, and ultimate purposes. For example, insulin and blood glucose levels should always be regarded as health data, whether it is collected by a caregiver at a clinic or by a patient through a diabetes mobile app, whether it is analyzed to evaluate the treatment effect or recorded to observe the development of diabetes, or whether it is ultimately for dividing different consumer groups or treating a particular patient.

Second, if the data fails the first step, it should be considered health data only to the extent that it is intended to be used when collected, or is actually used later on, to conduct health-related analysis, determine health-related correlations, draw health-related conclusions, or make health-related predictions. For example, one's diet pattern is nothing special if it is only used to record daily life activities and recommend a good lifestyle. However, the same diet pattern should be considered health data when used to evaluate your

---

[63] Joseph Conn, *IOM Panel Urges More EHR Collection of Social, Behavioral Data*, MODERN HEALTHCARE (Nov. 13, 2014, 12:00 AM), https://www.modernhealthcare.com/article/20141113/NEWS/311139943/iom-panel-urges-more-ehr-collection-of-social-behavioral-data [https://perma.cc/8GAM-NMVP].

[64] *Id.*

[65] *See generally* INST. OF MED., CAPTURING SOCIAL AND BEHAVIORAL DOMAINS IN ELECTRONIC HEALTH RECORDS: PHASE 1 (2014); INST. OF MED., CAPTURING SOCIAL AND BEHAVIORAL DOMAINS IN ELECTRONIC HEALTH RECORDS: PHASE 2 (2014).

[66] INST. OF MED., CAPTURING SOCIAL AND BEHAVIORAL DOMAINS IN ELECTRONIC HEALTH RECORDS: PHASE 1, 42 (2014).

risk of hypertension, no matter whether that risk evaluation is for purposes of diagnosing a particular disease by a caregiver or for rating health risks by an insurance company.

C. Big Health Data, Big Concerns

The expansion of health data is not always a blessing for consumers. If misused in combination with Big Data analytics, health data could operate against consumers' interests. The three main concerns to be discussed in this Section are: (1) psychological harms associated with unauthorized disclosure, (2) algorithmically imposed new discrimination threats, and (3) facilitation of fraud and identity theft because of easier data aggregation.

The first concern is the psychological harm associated with the unauthorized disclosure of sensitive personal information. Health data is recognized as the most private personal information.[67] Eighty-one percent of the respondents in a Pew survey believed that health data was "sensitive," with fifty-five percent considering it "very sensitive."[68] Dr. Richard Harding, a former president of the American Psychiatric Association, believes that disclosures of medical information could cause personal disgrace as well as discrimination;[69] he notes that:

> These disclosures can jeopardize our careers, our friendships, and even our marriages. And if such disclosures occur, there are truly few meaningful remedies. Seeking redress will simply lead to further dissemination of the highly private information that the patient wished to keep secret, nor can a financial settlement do much to compensate the individual for these highly personal losses. For all of these reasons, very tight restrictions on access as well as disclosure of medical records information is essential.[70]

Similarly, in enacting relevant privacy rules, HHS stated that a health privacy breach could cause significant impacts beyond one's physical health, including alienation of family and friends and public humiliation.[71] Granted,

---

[67] Zarsky, *supra* note 50, at 1012.
[68] Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 460–61 n.291 (2018).
[69] *Financial Privacy: Hearing on H.R. 10 Before the Subcomm. On Financial Institutions and Consumer Credit of the Comm. on Banking and Financial Services*, 106th Cong. 100 (1999) (statement of Donald J. Palmisano, M.D., J.D., A.M.A.), https://archive.org/details/financialprivacy00unit/page/n1 [https://perma.cc/26Z6-4LDM].
[70] *Id.*
[71] *See* Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1151 (2015).

people may have only traditional health data on their minds when responding to surveys and making comments and it is true that not all health data under this broadened Big Data definition carries the same level of sensitivity. Nevertheless, the underlying rationale is not limited to traditional health data. That is, people feel strongly about when, how, to whom, and to what extent their health data should be disclosed. They care about the resulting judgments made about their health problems and detriments to their reputations no matter if the information revealed is traditional health data or a result of combined health datasets.

In addition, because the resulting damages often extend beyond data subjects' expectations, misuse of health data in combination with Big Data analytics is probably even more psychologically harmful than misuse of health data in the traditional sense. What if the girl in the Target example above did not want her father to know about her pregnancy? She would of course be upset if her pregnancy was accidentally disclosed by a breach of her EHR, but she might be more distressed upon realizing that her purchasing data at Target turned out to be the information source.

Sharona Hoffman, a leading scholar in the areas of health information technology and civil rights, has noted another concern caused by Big Data analytics: the new health-related discrimination threats; employers, financial institutions, marketers, and educational institutions are all involved as potential stakeholders in this respect.[72] Data subjects could pay more for their health insurance plans, be denied certain financial transactions, and be excluded from certain products just because of the correlations and inferences arising from misuse of health data in the context of Big Data.[73] The White House raised the same concern in 2014 and pointed out that Big Data analytics could result in discriminatory use of personal information, endangering the civil rights protections in various domains including the healthcare sector.[74] If treatment, eligibility, inclusion, or access are determined by data, not only will

---

[72] See Sharona Hoffman, *Big Data's New Discrimination Threats: Amending the Americans with Disabilities Act to Cover Discrimination Based on Data-Driven Predictions of Future Disease*, *in* BIG DATA, HEALTH LAW, AND BIOETHICS 85, 85 (I. Glenn Cohen et al. eds., 2018) (noting that employers are keen to obtain prospective employees' medical information to determine whether they will develop serious illnesses for purposes of employment decisions; financial institutions are eager to collect individuals' health data to screen out applicants with a high risk of defaulting on loans because of medical difficulties; some educational institutions may be interested in applicants' health data to determine whether they are likely to have abbreviated careers and limited earnings because of medical challenges and become successful professors or otherwise bring honors to the institutions).

[73] *See* discussion *supra* Part II.B.

[74] *See* JOHN PODESTA ET AL., BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 45–47 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf [https://perma.cc/96S3-7TR6].

the well-established U.S. anti-discrimination values be significantly compromised, but also one's health, choices, life chances, and "general autonomy and human dignity"[75] may be undermined.

Worse, algorithmically imposed decisions about treatment or access may be based on correlations and inferences which are imperfect and can be easily misleading. Imagine you are studying issues related to multiple sclerosis (M.S.): You have conducted some online searches and subscribed to an online recommendation engine to look up physicians; then you receive an invite to a meeting of M.S. patients.[76] Why? Because some data handler has mistakenly profiled you as an M.S. patient and shared that profile with other marketers.[77] Wrong advertisements might only be annoying and superficially damaging, but if the recipient of an incorrect profile is an insurer or an employer with a discriminatory view against pre-existing conditions, the resulting harm could be more significant—you may lose a job opportunity or be denied a service based on a mistaken inference by a third-party, without your fault or knowledge.

Another emerging issue is Big Data's role in facilitating health related fraud and identity theft. Consider this example from 2007: A data broker named InfoUSA came up with a list of "Suffering Seniors" by aggregating health data about cancer and Alzheimer's disease, and sold it to telemarketers who targeted senior citizens.[78] Then the telemarketers raided those senior citizens' bank accounts by tricking them into revealing their bank information.[79] Even if the data transferred to perpetrators is insignificant, Big Data analytics makes it much easier for wrongdoers to devise similar lists and harm data subjects.

D. Under-regulated mHealth App Data

As one of the most significant groups of health data in the Big Data context, mHealth app data, unlike its counterparts in the traditional healthcare setting, currently receives no more protection than other consumer data. Because mHealth apps are mostly designed to fulfill health-related functions, such as treating diseases, managing chronic conditions, and promoting a

---

[75] Wolfie Christl, *How Companies Use Personal Data Against People* 17 (Working Paper by Cracked Labs, 2017), https://crackedlabs.org/dl/CrackedLabs_Christl_DataAgainstPeople.pdf [https://perma.cc/WB7S-6YV9].

[76] Natasha Singer, *When Your Data Wanders to Places You've Never Been*, N.Y. TIMES (Apr. 27, 2013), https://www.nytimes.com/2013/04/28/technology/personal-data-takes-a-winding-path-into-marketers-hands.html [https://perma.cc/MJ7U-UMB8].

[77] *Id.*

[78] Ashley Kuempel, *The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry*, 36 NW. J. INT'L L. & BUS. 207, 221 (2016).

[79] *Id.*

healthy lifestyle, the bulk of data generated by mHealth apps is intrinsically medically significant or is very likely to become health-related given the health-related context these apps are designed and used in. Accordingly, mHealth app data is overall more medically revealing and sensitive than consumer data from other sources. Baby kicks recorded by a pregnancy tracker app, for example, will always be a more direct source of data compared with Big Data inferences like Target's use of purchasing data discussed above.

However, because no regulation has been promulgated to provide extra protection, mHealth app data is, as with other consumer data, completely open to decontextualized, discriminatory, or criminal uses—as discussed earlier. Like data generated by other consumer-facing mobile apps, mHealth app data suffers from excessive collection from data subjects and under-regulated transmissions among app developers, data brokers, and other interested players.

Without compulsory standards, the only potential limitation is the notice-and-consent mechanism embedded in mobile apps' self-imposed privacy policies, breach of which, as discussed in Part III, triggers FTC's enforcement. However, most of these privacy policies are so one-sided that app developers can modify their terms at will and leave consumers with a consent-or-abandon choice.[80] In addition, privacy policies are usually long and complicated, and many users do not read or understand them prior to agreeing to the terms.[81]

Margaret Jane Radin, a leading legal scholar focusing on legal issues in cyberspace and exploring freedom of choice in the information society, has noted that "free consent involves a knowing understanding of what one is doing in a context in which it is actually possible for one to do otherwise, and an affirmative action in doing something, rather than a merely passive acquiescence in accepting something."[82] Unfortunately, free consent is difficult to find in many consumer-facing apps including mHealth apps. Although questions remain about the best way to seek consumers' consent, be it the traditional notice-and-consent mechanism or the opt-in and opt-out approaches, the chosen method should allow users to make meaningful choices, instead of operating as a shield for potential privacy violations.

Moreover, some mHealth apps, together with many other consumer apps, do not even have privacy policies. It is reported that approximately twenty six percent of free mobile apps and forty percent of paid health mobile

---

[80] Fred H. Cate & Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data*, 3 INT'L DATA PRIVACY LAW 67, 67 (2013).

[81] *See e.g.*, J. Frazee et al., *mHealth and Unregulated Data: Is This Farewell to Patient Privacy*, 13 IND. HEALTH L. REV. 384, 407 (2016).

[82] Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1125–26 (1999).

apps do not have privacy policies.[83] Another survey indicates that only about thirty percent out of the six hundred most-used mHealth apps had privacy policies.[84] In addition, most data brokers, as the primary downstream players, do not set any contractual obligations with their data sources to ensure that they or their counterparties provide consumers with notice of information sharing with third-parties and an opportunity to opt out of such sharing.[85] In conclusion, the whole industrial chain is taking advantage of the current liberal regulatory environment.

What is more worrisome is that mHealth app data is more "popular" on the market, and therefore more liable to misuses. First, compared with other consumer apps, health and fitness apps sent sensitive data to more third-party domains.[86] FTC's earlier study revealed that twelve mHealth apps and devices transmitted information to seventy-six different third parties without consumers' knowledge, with eighteen third parties receiving device-specific identifiers, fourteen receiving consumer-specific identifiers, and twenty-two receiving other key health data.[87]

Second, in contrast with other consumer data, mHealth app data is more likely to become a pricy "commodity" on the market: Its price is ten times that of other personal data on the data market,[88] and is fifty times that of credit card information on the black market.[89]

Some may argue that mHealth app data does not necessarily have major sensitivities because data can be de-identified. This is largely unfounded. First and foremost, there are few proper regulations for the collection, transmission and transaction of mHealth app data, much less a statutory requirement for its de-identification. Second, even if a single set of mHealth app data is de-identified, re-identification is not a difficult task when analyzed in conjunction with other datasets, thanks again to Big Data analytics.[90] For example, the latest findings show that by matching daily step data collected by activity trackers, smartwatches, and smartphones to

---

[83] Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 439 (2018).
[84] Guadarrama, *supra* note 29, at 1016.
[85] FED. TRADE COMM'N, *supra* note 58, at 16.
[86] Jinyan Zang et al., *Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps*, TECH. SCI. 1, 17 (2015), https://techscience.org/a/2015103001/download.pdf [https://perma.cc/8TE3-R9PA].
[87] Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. B. 76, 77 (2016).
[88] Lashbrook, *supra* note 2.
[89] Andrews, *supra* note 68, at 431.
[90] *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1717–22 (2010).

demographic data, individuals can be re-identified.[91] So it is possible for Facebook to re-identify you if it gathers your step data from your mHealth app, buys another set of data from another company, and then matches the two datasets.[92]

In conclusion, compared with other consumer data, mHealth app data is generally more sensitive, more revealing, and more liable to Big Data misuse against the interests of data subjects and yet they are in an almost regulation-free zone.

III. CURRENT FEDERAL STATUTORY LANDSCAPE AND GAPS

Commentators have criticized the U.S. data protection legal system as "fragmented,"[93] "patchwork,"[94] and "haphazard."[95] These criticisms are based on the fact that there is no unified, baseline protection statute for consumer data on the federal level. Under the existing legal framework, whether privacy problems can be addressed mainly depends on the industry at issue and the actors involved.[96]

As discussed earlier, the primary federal regulators of mHealth apps are HHS, FDA, and FTC, but no single regulator has complete jurisdiction over mHealth app data. HIPAA only regulates "protected health information" (PHI) to the extent that it is held by HIPAA-defined covered entities and business associates, but many users and processors of mHealth app data do not meet HIPAA's definitions of covered entities and business associates. Also, HIPAA does not regulate health data collection, despite excessive collection being a primary concern for mHealth app data. FDA, on the other hand, focuses its oversight on the efficacy and safety of mHealth apps, and does not regulate privacy issues. Lastly, FTC, relying on Section 5 of the Federal Trade Commission Act (FTC Act), is now an active regulator for mHealth app data, but its authority is limited, unclear, and liable to challenges.

---

[91] *Artificial Intelligence Advances Threaten Privacy of Health Data,* EUREKALERT! (Jan. 3, 2019), https://www.eurekalert.org/pub_releases/2019-01/uoc--aia010319.php [https://perma.cc/UKP6-TEJV].

[92] Jessica Kim Cohen, *AI Can Re-Identify De-Identified Health Data, Study Finds*, BECKER'S HEALTH IT & CIO REP. (Jan. 3, 2019), https://www.beckershospitalreview.com/artificial-intelligence/ai-can-re-identify-de-identified-health-data-study-finds.html [https://perma.cc/5H4V-EAQJ].

[93] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

[94] Helm & Georgatos, *supra* note 15, at 140.

[95] Ohm, *supra* note 71, at 1140.

[96] Helm & Georgatos, *supra* note 15, at 140.

Because FDA is not currently engaged in privacy issues, the following Section will only discuss the regulatory approaches adopted by HIPAA and FTC, and their flaws.

A. HIPAA: A Closed, Downstream Approach

The most well-known federal statute for health data protection is HIPAA.[97] After several amendments and updates, the existing HIPAA rules (HIPAA Rules) are primarily composed of the Privacy Rule, the Security Rule, and the Breach Notification Rule, incorporating relevant requirements posed by other acts such as the Health Information Technology and Economic Clinical Health Act (HITECH Act).[98]

Promulgated with several purposes such as combating health care fraud and improving access to insurance coverage,[99] HIPAA was initially silent on health data protection; instead, HHS was delegated to issue separate regulations to protect personal health information absent a Congressionally enacted comprehensive privacy legislation within three years of HIPAA's enactment.[100] Therefore, when Congress missed its deadline, HHS promulgated the Privacy Rule in 2002 and the Security Rule in 2003.[101] The HITECH Act, enacted in 2009, strengthened HIPAA's protection by expanding the definition of business associate, extending application of the Privacy Rule and the Security Rule to business associates,[102] and incorporating new breach notification requirements.[103] On January 25, 2013, by publishing the HIPAA Omnibus Rule, HHS further incorporated the relevant data

---

[97] There are some other statutes regulating use of health data, but they are more focused on prevention of health-based discrimination by certain specified actors, rather than regulating the flow of health data. Therefore, this Article does not examine these statutes. For example, the Genetic Information Nondiscrimination Act (GINA) of 2008 protects Americans from discrimination based on their genetic information by health insurers and employers. The Americans with Disabilities Act (ADA) prohibits discrimination against individuals with disabilities in areas of public life, such as jobs, schools, and transportation. *See* Genetic Information Nondiscrimination Act, Pub. L. No. 110-233, 122 Stat. 881–922 (2008); Americans with Disabilities Act of 1989, Pub. L. No. 101-336, 104 Stat. 327–378 (1989).

[98] U.S. DEP'T OF HEALTH & HUMAN SERVS., EXAMINING OVERSIGHT OF THE PRIVACY & SECURITY OF HEALTH DATA COLLECTED BY ENTITIES NOT REGULATED BY HIPAA 12 (2016), https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf [https://perma.cc/XB3P-D4XD].

[99] Stacey A. Tovino, *The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons*, 47 SETON HALL L. REV. 973, 975 (2017).

[100] *Id.* at 976.

[101] STEPHEN S. WU, A GUIDE TO HIPAA SECURITY AND THE LAW 2 (2d ed. 2016).

[102] Nicolas Terry, *Health Privacy is Difficult but Not Impossible in a Post-HIPAA Data-Driven World*, 146 CHEST 835, 836 (2014).

[103] *Id.*

protection provisions of the HITECH Act and the Genetic Information Nondiscrimination Act (GINA) into the HIPAA Rules.[104]

The HIPAA Rules regulate the flow of PHI within a closed community among individuals, covered entities, and business associates. Some definitions are needed to better understand the HIPAA mechanism.

As used in the HIPAA Rules, PHI means information relating to an individual's health conditions, health care received, or health care related payment that (1) is created or received by covered entities or business associates, and (2) identifies or can be reasonably used to identify such individual.[105] De-identified health information is thus not protected.[106] "Covered entity" includes a health plan, a health care clearinghouse, or a health care provider who transmits electronic health information in relation to a HIPAA-covered transaction;[107] "business associate" refers to: (1) a person providing PHI transmission services to a covered entity and requiring routine access to PHI, (2) a person offering personal health records to individuals on behalf of a covered entity, and (3) a subcontractor that deals with PHI on behalf of the business associate.[108]

To the extent that PHI is held by a covered entity or a business associate, the HIPAA Rules provide relatively robust protections in the sense that data subjects can obtain and correct their PHI; can know, designate, and limit their PHI's recipients; and can be informed of and complain about breaches of PHI.[109] Specifically, data subjects' written authorizations from individuals must be obtained before use or disclosure of their PHI,[110] except that PHI may be used or disclosed without individuals' authorization[111] for

---

[104] Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566 (proposed Jan. 25, 2013) (to be codified at 45 C.F.R. § 160 and 164).

[105] 45 C.F.R. § 160.103 (2019).

[106] U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 4 (2013), https://www.hhs.gov/sites/default/files/privacysummary.pdf [https://perma.cc/A7CL-F844].

[107] 45 C.F.R. § 160.103 (2019).

[108] *Id.*

[109] U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 98, at 14.

[110] *Id.*

[111] U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 98, at 14; *but see* INST. OF MED., CAPTURING SOCIAL AND BEHAVIORAL DOMAINS IN ELECTRONIC HEALTH RECORDS: PHASE 2 325–326 (2014) (noting that psychotherapy notes recorded in any medium by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session are separated from the rest of the individual's medical record. A covered entity is required to obtain the patient's express written authorization for any use or disclosure of psychotherapy notes, except for the following: (1) the treatment uses by the originator of the notes; (2) use or disclosure in mental

HIPAA-permitted purposes such as health care operations[112] and public health activities.[113]

Also, HIPAA embraces a principle of "minimum necessary" disclosure.[114] Unless under specified circumstances, a covered entity or business associate is required to "make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request."[115] These robust protections do not function well when applied to mHealth app data for two reasons.

First, mHealth app data—however sensitive—is not subject to HIPAA's governance because mHealth apps are consumer-grade products not typically offered by a covered entity or business associate.[116] The fundamental issue under HIPAA is that the custodians of the data matter more than the data itself.[117] That is, whether an individual's health data is protected by HIPAA depends on *who* is holding the data, rather than *what* the data is.[118] HIPAA focuses on how health data should be channeled, instead of how the private interests attached to health data should be safeguarded.[119]

This custodian-centric approach has led to two unreasonable scenarios. First, health data of the same nature may receive different treatment as a result of the different settings where it is processed. For instance, a patient's glucose level measured at a brick-and-mortar healthcare provider, such as a clinic or a

---

health professional training programs; (3) use by the covered entity to defend itself in a lawsuit brought by the individual who is the subject of the notes; (4) disclosures required by law; (5) uses related to oversight of the originator of the notes; (6) disclosures to coroners and examiners to help determine cause of death; and (7) disclosures to prevent an imminent threat to health or safety).

[112] 45 C.F.R. § 164.501 (2019) ("Health care operations" include a covered entity's various activities necessary to run its business and to support the core functions of treatment and payment, such as quality assessment and improvement activities, internal performance evaluation, medical review, legal services, auditing functions, business planning and development, business management and general administrative activities).

[113] 45 C.F.R. § 164.512 (2019) (A covered entity may use or disclose PHI for the purpose of public health activities. For example, a covered entity may disclose PHI to a public health authority for purpose of preventing or controlling disease, injury, or disability and receiving reports of child abuse or neglect or disclose to FDA-governed persons for the purpose of activities related to the quality, safety or effectiveness of FDA-regulated products or activities).

[114] 45 C.F.R. § 164.502(b) (2019).

[115] *Id.* (For example, the minimum necessary standard does not apply to disclosures by a health care provider for treatment purposes, or disclosures permitted or compelled by applicable law).

[116] Guadarrama, *supra* note 29, at 1005.

[117] *See* Terry, *Regulatory Disruption*, *supra* note 49, at 164.

[118] U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 98, at 12.

[119] Theodore Rostow, *What Happens When an Acquaintance Buys Your Data: A New Privacy Harm in the Age of Data Brokers*, 34 YALE J. REG. 667, 677 (2017).

hospital, is protected by HIPAA. However, if the patient enters the same dataset into an mHealth app at home, the data is not protected under HIPAA.

Second, HIPAA-protected health data may lose its protection solely due to a change of hands. If consumers use a third-party health management app that is not offered or otherwise in association with their healthcare providers and then add certain health data from their HIPAA-protected EHR to that app, that health data is now outside the reach of HIPAA.[120] This counterintuitive outcome is related to HIPAA's initial legislative intention. Initially, HIPAA was promulgated to standardize the electronic exchange of health data involved in financial and administrative transactions covered by HIPAA. Privacy protection was not initially included within the statute.[121] Consequently, the focus of the HIPPA Rules on the doctor-hospital-insurer ecosystem is natural. In a traditional healthcare system, doctors, hospitals and insurers—as the data holders captured by the HIPAA—are almost the only players. It seems sufficient for lawmakers to only regulate conducts of these players. Therefore, the regulatory gap before the emergence of mHealth products was not that significant. Currently, mHealth technology is reshaping the healthcare sector and has presented new issues as to (1) under what circumstances and for what purposes health data is collected, transmitted and processed, and (2) who has the opportunity and right to touch and control health data. HIPAA's custodian-centric approach needs to be updated—if not abandoned—in order to respond to these new issues.

HIPAA's second flaw is that it only regulates the flow of health data, not its collection.[122] Nicolas P. Terry, a widely recognized leading academic in the field of health information and technology laws, describes this privacy protection approach as a "downstream" model, which only seeks to contain the collected data within the healthcare system by prohibiting its transmission to non-health-care parties, but imposes no limitation on data collection at the outset.[123] Terry traces this to the traditional culture of medicine, which favors collecting as much information as possible.[124] The rationale is that universal collection and free flow of health data could maximize patient health and achieve more public health goals.[125] This suggests a lag in regulatory rationale in the face of new information technologies.

---

[120] Timothy Newman & Jennifer Kreick, *The Impact of HIPAA (and Other Federal Law) on Wearable Technology*, 18 SMU SCI. & TECH. L. REV. 429, 446 (2015).
[121] WU, *supra* note 101, at 2.
[122] Nicolas Terry, *Health Privacy is Difficult but Not Impossible in a Post-HIPAA Data-Driven World*, 146 CHEST 835, 837 (2014).
[123] *Id.*
[124] Terry, *supra* note 49, at 165.
[125] Terry, *supra* note 57, at 68.

Data collection may not be a major concern if healthcare is only conducted by traditional healthcare providers in a "simple health-care data exchange scenario"[126] that is already supported by confidentiality rules in exchange for more effective treatment.[127] A patient sitting in front of a physician knows exactly what information is being collected and does not need to worry about unnecessary data collection. However, data collection becomes a problem when data is collected by mHealth apps. mHealth apps have broadened the scope of data collection, and users are often in the dark about what data is being collected, who is collecting it, and how it is being used. An mHealth app could—if turned on by a person and left without interruption—collect an abundance of data and "achieve 24/7 monitoring in order to create a digital doppelganger of the person."[128] The scope of data collection further expands when an app goes beyond its proclaimed purpose and unnecessarily collects users' other data such as geolocation, contact lists, or search history—as is often the case. This over-collection concern would not be addressed by the current HIPAA Rules even if those rules did cover mHealth app data because the HIPAA Rules have no complementary limit on data collection despite its existing requirement for minimization of data sharing.

B. FTC's Section 5 Power: Only If You Break Your Promise

Because the HIPAA Rules cannot capture most mHealth app data, and FDA is hands-off to protection of mHealth app data, FTC is becoming a leading regulator in this field.[129] HHS acknowledges that the FTC Act[130] is currently the primary federal statute regulating health data not covered by HIPAA.[131]

FTC's authority to regulate mHealth app data stems from its general power to protect consumer privacy under Section 5 of the FTC Act.[132] FTC's Section 5 power extends to persons, partnerships, or corporations, except banks, savings and loan institutions, federal credit unions, common carriers, air carriers, and packers that are subject to specialized laws and regulations.[133] Therefore, all data handlers, whether covered by HIPAA or not, are subject to Section 5 as long as they do not fall into one of those exceptional categories.

---

[126] Terry, *supra* note 49, at 165.
[127] *Id.*
[128] Andrews, *supra* note 68, at 426.
[129] Hartzog & Solove, *supra* note 16, at 2267.
[130] Federal Trade Commission Act, 15 U.S.C. §§ 41–58 (2018).
[131] U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 98, at 17.
[132] Solove & Hartzog, *supra* note 93, at 604.
[133] 15 U.S.C. § 45(a) (2018).

Instead of focusing on data's intrinsic characteristics or data protection,[134] FTC's Section 5 authority prevents an entity "from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[135] To justify its power to enforce privacy protection, FTC reasons that false or misleading promises about privacy and security or inadequate security measures are likely to injure consumers, and should therefore be covered by Section 5.[136]

According to FTC, unauthorized access to information by an app in violation of its app's own privacy policies is "deceptive,"[137] and an app's failure to maintain adequate data security is simply "unfair", regardless of its own data security promise.[138]

In enforcing Section 5, FTC has developed some general data protection principles, which include (1) adhering to promised privacy practices; (2) informing data subjects of uses and disclosures of material personal information; (3) notifying data subjects of data sharing with third parties outside the direct consumer relationship; (4) implementing reasonable and appropriate security measures; and (5) safeguarding private information based on the type of information and the risk presented to consumers.[139]

If FTC reasonably believes that any person is engaging in any unfair or deceptive act or practice, FTC may initiate a hearing upon serving on the person a complaint and a notice of a hearing;[140] if the person complained of fails to justify its act or practice at the hearing, FTC may then make a written report and issue a cease and desist order.[141] The person receiving a cease and desist order may petition for a review of that order by a competent court, and the court may then affirm, modify, or setting aside FTC's order, and enforce the same to the extent that such order is affirmed.[142]

However, FTC's Section 5 authority is limited. For a deceptiveness prong claim, FTC follows a "broken promises" approach.[143] That is, only when an app developer makes false or misleading claims about its privacy or

---

[134] Terry & Gunter, *supra* note 47, at 139.
[135] Helm & Georgatos, *supra* note 15, at 159.
[136] Guadarrama, *supra* note 29, at 1011.
[137] Helm & Georgatos, *supra* note 15, at 160.
[138] Hartzog & Solove, *supra* note 16, at 2275.
[139] MAXIMUS FED. SERVS., NON-HIPAA COVERED ENTITIES: PRIVACY AND SECURITY POLICIES AND PRACTICES OF PHR VENDORS AND RELATED ENTITIES REPORT 3–4 (2012), https://www.healthit.gov/sites/default/files/maximus_report_012816.pdf [https://perma.cc/Y73U-RXJK].
[140] Federal Trade Commission Act, 15 U.S.C. § 45(b) (2018).
[141] *Id.*
[142] 15 U.S.C. § 45(c) (2018).
[143] ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 82 (2018).

data security procedures can FTC trigger an enforcement action. Because there is currently no compulsory standard or robust self-regulation regime for privacy policies and security measures in the mHealth app industry, app developers can decide how they draft their own privacy policies and formulate security procedures. If they choose to set a lower bar, FTC has no power to impose a higher one.

Compared to the limited—but straightforward—"broken promises" approach, claims under the unfairness-prong appear more challenging because the standard of proof is high. FTC must prove that (1) the practice in question has caused or is likely cause significant harms to consumers, (2) such harms cannot be reasonably avoided by customers, and (3) such harms are not outweighed by the resulting benefits.[144]

FTC has used this three-part test to take enforcement actions against companies that have poor data security practices regarding health data,[145] but not always with success.[146] The U.S. Court of Appeals for the Eleventh Circuit recently struck down FTC's cease and desist order against LabMD, a cancer detection facility holding sensitive health data.[147] Because one of LabMD's employees used a file-sharing app and inadvertently made available health data to third parties, a hacker company managed to access sensitive information of about 9,000 patients.[148] FTC investigated and asserted in its complaint that LabMD's data security practices were "unreasonably lax," making them unfair under Section 5.[149]

The court found that FTC failed to cite explicitly the source of the standard of unfairness and failed to specify the unfair acts or practices engaged in by LabMD.[150] Although fact-specific, the court's holding indicates that compared with the deceptiveness prong claim, the standard of proof of the unfairness prong claim is higher and requires FTC to stretch its interpretation of Section 5 even further to justify its enforcement actions.

As the leading, catchall regulator of privacy-related practices of mobile apps, FTC seems to be in a good position to regulate mHealth app data. However, because the FTC Act does not explicitly grant FTC the authority to

---

[144] 15 U.S.C. § 45(n) (2018).
[145] U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 98, at 18.
[146] *See FTC Rebuked in LabMD Case: What's Next for Data Security?*, WILEY REIN LLP (Jun. 7, 2018), https://www.wileyrein.com/newsroom-articles-FTC_Rebuked_in_LabMD_Case_Whats_Next_for_Data_Security.html [https://perma.cc/5WU6-MY3U].
[147] *Id.*
[148] *Id.*
[149] *Id.*
[150] LabMD, Inc. v. Fed. Trade Comm'n, 894 F.3d 1221, 1230–31 (11th Cir. 2018).

protect privacy,[151] the effect of FTC's regulation is limited. The deceptiveness prong ultimately counts on industry players' self-discipline, and the unfairness prong relies on FTC's stretched interpretation of "fairness," neither of which are guaranteed by any rulemaking power or enforceable, compulsory standards. Unless these limitations are overcome, FTC is not ready to completely address the privacy concerns posed by mHealth app data.

IV. GAP-FILLING PROPOSALS

A. Necessity of Governmental Action to Address Regulatory Gaps

The next inquiries are: Do these regulatory gaps need to be addressed? If so, how? On the general topic of consumer privacy protection, views differ as to whether privacy protection could best be achieved through agency regulation or self-regulation.[152] There are two major arguments supporting the self-regulation approach. First, regulation for privacy protection is not worth discussing, as people either no longer have expectations of privacy or are willing to exchange privacy for more significant benefits. Second, self-regulation is sufficient for privacy protection and there is no need for any government-involved regulation. This Part will examine and counter these two arguments in turn.

1. *Privacy in the Digital Age: Shifted Expectations or Trade-off?*

Many doubt the intrinsic value of privacy in the digital age, [153] and ask whether regulation of any form is needed at all. This Section argues that the expectations of privacy have shifted over time, but this shift has not led, and should not lead, to the demise of privacy in the digital age.

Those opposed to privacy rights might base their propositions on the assumption that privacy is somewhat equal to secrecy and ends when disclosure is made. Under their reasoning, because data collection, disclosure, aggregation, and analysis are inevitable in the digital age, there is no way to

---

[151] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-13-663, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 11 (2013), https://www.gao.gov/assets/660/658151.pdf [https://perma.cc/FV5R-G59C].

[152] *Id.* at 16.

[153] *See, e.g.*, Peter Friedman, *Is Privacy Dead in The Digital Age? What To Do About It: Part I,* MEDIAPOST (July 26, 2018), https://www.mediapost.com/publications/article/322686/is-privacy-dead-in-the-digital-age-what-to-do-abo.html [https://perma.cc/E38D-Y63W].

hide information forever, and the protection of privacy as a right is therefore questionable.[154]

Alternatively, privacy opponents might argue that although privacy remains of significant value, there is, at least in the digital world, a trade-off about privacy.[155] Consumers are willing to sacrifice their data and privacy in exchange for considerable benefits,[156] such as increased economic efficiency, improved security, better personalization of services, increased availability of information, innovative platforms for communication,[157] and free services. In other words, data subjects are willing to accept, and have accepted, the costs incurred due to the technological advancements, and do not care about privacy as much as advocates and regulators believe. For example, in a survey of over 4,000 individuals about online purchases, sixty-five percent of the respondents reported that they seldom read privacy policies.[158] This seems to show consumers' indifference to privacy. Those opposed further reason that, now that consumers' expectations and notions of privacy have changed, there is no need for strict privacy control mandated by law.[159] The next Section provides some theoretical and empirical counterarguments to this anti-privacy perspective.

a. Shifted Expectations of Privacy

The doubters of privacy rights miss the mark because they regard privacy as a static notion. They have failed to consider another general proposition from the famous article by Samuel Warren and Louis Brandeis: "Political, social and economic changes entail the recognition of new rights."[160] The right to privacy, like all other rights, is ever-changing, but has never faded. At first, we had privacy in physical space, and then privacy relating to making choices, and now, information privacy[161] as a right to

---

[154] Art Caplan, *Why Privacy Must Die*, HEALTH CARE BLOG (Dec. 19, 2016), https://thehealthcareblog.com/blog/2016/12/19/goodbye-privacy-we-hardly-knew-ye/ [https://perma.cc/KX7P-UZLD].

[155] *See, e.g.*, Jon Reily, *Privacy or Convenience: What's the Tradeoff?*, PUBLICIS SAPIENT, https://www.publicissapient.com/insights/privacy-or-convenience--what-s-the-tradeoff [https://perma.cc/T4VV-2DN9].

[156] Frazee et al., *supra* note 81, at 409.

[157] Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms, and Consent*, 14 J. HIGH TECH. L. 370, 385 (2014).

[158] Frazee et al., *supra* note 81, at 393 n.46.

[159] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 151, at 27.

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

[161] *See* INST. OF MED., HEALTH DATA IN THE INFORMATION AGE: USE, DISCLOSURE, AND PRIVACY 143–54 (1994), (providing a review of the concept of privacy in America, and noting that the development of the concept of privacy in the U.S. encompasses three clusters of ideas:

privacy in the sharing of personal information.[162] Best depicted by the eight "Fair Information Practice Principles" (FIPPs) adopted in the 1970s, the contents of informational privacy include openness, individual access, individual participation, collection limitation, use limitation, disclosure limitation, information management, and accountability.[163]

Entering the digital age, many commentators have posited structured elaborations of the right to privacy from various perspectives. Alan Westin, a pioneering legal scholar and political scientist in the field of consumer data privacy and data protection, associates privacy with one's control over personal information and defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[164]

Jack Balkin, a prominent legal scholar in the field of Constitutional law and new information technologies, approaches the right to privacy with a focus on relationship.[165] He has put forward the concept of an "information

(1) decisional privacy, which embodies autonomy interests concerning the exercise of fundamental constitutional liberties with respect to private behavior, such as decisions relating to marriage, procreation, contraception, family relationships, and child-rearing; (2) spatial privacy, which protects people against surveillance or intrusion such as unlawful searches of one's home or person and unauthorized wiretapping; and (3) informational privacy, which represents an individual's control over the dissemination, use, and access by others of information that relates to himself or herself); *see also* NAT'L RESEARCH COUNCIL, ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE 58–87 (2007) (going through the long intellectual history of the notion of privacy in the United States from the perspectives of philosophy, economics, and sociology).

[162] Elizabeth A. Rowe, *Sharing Data*, 104 IOWA L. REV. 287, 301 (2018), https://ilr.law.uiowa.edu/print/volume-103-issue-6/sharing-data/ [https://perma.cc/BP9K-E6VN].

[163] Griffin Drake, *Navigating the Atlantic: Understanding EU Data Privacy Compliance Amidst a Sea of Uncertainty*, 91 S. CAL. L. REV. 163, 167 (2017), https://southerncalifornialawreview.com/2017/11/01/navigating-the-atlantic-understanding-eu-data-privacy-compliance-amidst-a-sea-of-uncertainty-note-by-griffin-drake/ [https://perma.cc/4VN6-RBWK].

[164] *See* NAT'L RESEARCH COUNCIL, ENGAGING PRIVACY AND INFORMATION TECHNOLOGY IN A DIGITAL AGE 59 (2007).

[165] *See* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C.D. L. Rev. 1183, 1234 (2016) (arguing that new classes of digital information fiduciaries should be created to require platform owners to respect the free speech and privacy of end users in return for special legal status and benefits); *see also* Benjamin Wittes & Wells C. Bennett, *Databuse and a Trusteeship Model of Consumer Protection in the Big Data Era*, BROOKINGS: GOVERNANCE STUD. (2014), https://www.brookings.edu/wp-content/uploads/2016/06/Wittes-and-Bennett_Databuse.pdf (proposing a negative right to privacy based on "trusteeship" and expectations of no "databuse," which is defined as "the malicious, reckless, negligent, or unjustified handling, collection, or use of a person's data in a fashion adverse to that person's interests and in the absence of that person's knowing consent") [https://perma.cc/SCP2-49VL].

fiduciary" to define certain non-contractual, relationship-based duties of data service providers towards data subjects.[166] Similar to other professional relationships, such as the lawyer-client relationship and the physician-patient relationship, these fiduciary duties would require data service providers to, even absent an express contractual promise, act in the best interest of data subjects.[167] Specifically, this means information fiduciaries could not use information obtained in the course of the relationship to the disadvantage of data subjects or to create conflicts of interest with data subjects.[168]

Ari Ezra Waldman, a leading thought leader on online privacy and safety, frames privacy as a trust-based social norm and argues that "we should conceptualize information privacy in terms of relationships of trust and leverage law to protect those relationship."[169]

Helen Nissenbaum, who has developed the "contextual integrity" theory, associates adequate privacy protection with norms of specific contexts.[170] In her view, the gathering, dissemination, and use of data should be context-specific, and the governing norms of distribution within different contexts should be obeyed.[171]

European scholars go even further to propose a "legitimate interest" argument. They argue that privacy is adequately protected if a legitimate interest is served in favor of data subjects in all stages of the life cycle of personal data, including collection, use, further use, and destruction.[172]

---

[166] Balkin, *supra* note 165, at 1234.

[167] *Id.*

[168] *See id.*

[169] WALDMAN, *supra* note 143, at 4–5; *see also* Eugenio Mantovani et al., *Towards a Code of Conduct on Privacy for mHealth to Foster Trust Amongst Users of Mobile Health Applications*, DATA PROTECTION AND PRIVACY: (IN)VISIBILITIES AND INFRASTRUCTURES 81, 84 (Ronald Leenes et al. eds., 2017) (noting that privacy is based on the trust that the other party will behave responsibly and will not attempt to exploit the vulnerabilities of the user).

[170] *See* Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 158 (2004); *see also* Helen Nissenbaum, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010) (proposing a model of informational privacy where contextual integrity is adopted as the benchmark for prescribing restrictions on the collection, use, and dissemination of information, variables of which include the nature of the context, the nature of the information in relation to that context, the roles of agents receiving information and their relationships with information subjects, and how the information is shared and further disseminated).

[171] *Id.*

[172] *See generally* Lokke Moerel & Corien Prins, *Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things*, SSRN ELEC. J. (2016), https://papers.ssrn.com/abstract=2784123 (asking whether the existing purpose-centric EU legal regime is effective and legitimate in a future driven by data, and proposing a legitimate interest test where regulations will not determine the conditions for which data processing is allowed, but will only set standards in cases where data are used in a manner that should be qualified as abuse) [https://perma.cc/D4MC-4Z7S].

Together, these different theories of privacy indicate that scholarly and individual perceptions of privacy lie on a spectrum. This Section does not attempt to argue that we should place mHealth app data on any particular point on that spectrum. Instead, it argues that these doctrinal efforts have reflected the shifted expectations of privacy and have defeated the argument that the right to privacy has been vitiated.

b. Trade-off as a Fallacy

The privacy trade-off argument proves to be a fallacy as well.[173] Most adults, as reported by Harris Poll, are willing to allow people to access and use their personal information only to the extent that they know the reasons for data use, see the tangible benefits for doing so, and believe care is taken to prevent misuse.[174] A 2015 Nielsen survey revealed that fifty-three percent of respondents were concerned that their data might be shared without their knowledge.[175] Although these surveys seem to be conducted on a debatable assumption that personal data is property owned and controlled by data subjects,[176] it is at least fair to conclude from these surveys that, in principle, people are both cautious about how their personal data is transmitted and used and afraid of the risks and harms associated with the unexpected misuse of personal data.

Why, however, do some surveys suggest that users are indifferent to their personal data? This gap, termed by some as the "privacy paradox," results from several factors, including unawareness, resignation, psychological distortions, and overestimation of existing protections. [177]

Both unawareness and resignation arise out of information asymmetry. As discussed earlier, due to the complexity of data processing technologies

---

[173] *See generally* JOSEPH TUROW ET AL., THE TRADEOFF FALLACY: HOW MARKETERS ARE MISREPRESENTING AMERICAN CONSUMERS AND OPENING THEM UP TO EXPLOITATION (Annenberg School for Communication ed., 2015) (going beyond the cost-benefit analyses and discussing the issues such as resignation and information asymmetry).

[174] Sloan & Warner, *supra* note 157, at 384–85.

[175] *See* Elizabeth A. Brown, *The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work*, 16 YALE J. HEALTH POL'Y L. & ETHICS 1, 10 (2016).

[176] *See, e.g.*, I. Glenn Cohen, *Is There a Duty to Share Healthcare Data*?, *in* BIG DATA, HEALTH LAW, & BIOETHICS 209 (I. Glenn Cohen et al., eds., 2018); Jorge L. Contreras & Francisca Nordfalk, *Liability (and) Rules for Health Information*, 29 HEALTH MATRIX 179 (2019); Mark Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J. L. & MED. 586 (2010).

[177] *See e.g.*, Sonja Utz & Nicole C. Krämer, *The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms*, 3 CYBERPSYCHOLOGY: J. OF PSYCHOL. RES. ON CYBERSPACE (2009), https://cyberpsychology.eu/article/view/4223 [https://perma.cc/7V6P-LEXQ].

and unfriendly, take-it-or-leave-it style privacy policies,[178] users know little about how privacy policies apply to their personal data[179] or the alternatives available to them. As a result, users may feel forced to sacrifice privacy[180] and resigned to giving up control of their data.[181] Back in the 1990s, Jeffrey Rothfeder perfectly described the feeling of powerlessness in the face of privacy intrusion:

> Increasingly, people are at the whim of not only pressure groups, but also large organizations - direct marketers, the credit bureaus, the government, and the entire information economy - that view individuals as nothing but lifeless data floating like microscopic entities in vast electronic chambers, data that exists [sic] to be captured, examined, collated, and sold, regardless of the individual's desire to choose what should be concealed and what should be made public.[182]

Information asymmetry has limited users' ability to make choices and take actions in accordance with their true desire to protect privacy.[183]

Furthermore, as indicated by research in social psychology and behavioral economics, even having all the information necessary for an informed choice, one would sometimes end up behaving against better judgment due to the plight of immediate gratification.[184] As long as the privacy threat is not imminent, it is easier for most people to accept a default choice already made for them rather than to make a different choice, even if the default is less advantageous.[185]

---

[178] Sloan & Warner, *supra* note 157, at 400.
[179] Nicolas A. Ozer, *Putting Online Privacy above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 224 (2012).
[180] Patrick Myers, *Protecting Personal Information: Achieving a Balance between User Privacy and Behavioral Targeting*, 49 U. MICH. J. L. REFORM 717, 731 (2016).
[181] TUROW ET AL., *supra* note 173, at 3.
[182] INST. OF MED., *supra* note 161, at 138 (quoting JEFFERY ROTHFEDER, PRIVACY FOR SALE (1992)).
[183] TUROW ET AL., *supra* note 173, at 3.
[184] Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification*, *in* PROCEEDINGS OF THE 5TH ACM CONFERENCE ON ELECTRONIC COMMERCE 21, 24 (2004), https://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf (stating the plight of immediate gratification when users face privacy sensitive decisions, they hardly have all information necessary for an informed choice; however, even if they had, they would be likely unable to process it and even if they could process it, they may still end behaving against our own better judgment) [https://perma.cc/3AYL-EAE5].
[185] NAT'L RESEARCH COUNCIL, *supra* note 164, at 76.

The last, ironic reason for this paradox is that users often overestimate the protections available to them.[186] Some assume that a privacy policy is sufficient. For example, sixty-five percent of the responding users reported believing that having a privacy policy meant that the service provider would not share their information with others without their permission.[187] Others believed that if they paid a fee, their privacy protection would be guaranteed.[188] However, paid mHealth apps are found to be no better than free apps in terms of data collection and sharing.[189]

Some may further question that if people really value privacy, why are products with enhanced privacy protections not dominating the market. The quick answer is that the privacy paradox has in turn hindered the development of a healthy market and rendered the market test ineffective. Consumers are simply stuck in this privacy paradox. Without sufficient demands for privacy-protecting goods and services, the market share of such products remains too small to make any impact.[190]

To sum up, there are many doctrinal efforts and empirical studies around privacy going on. It can be concluded that individuals' expectations of privacy remain, but information asymmetry and psychological limitations have distorted consumers' true desire and hindered the formation of a healthy market. That is exactly why we need regulation to correct the distortion.

2. *The Illusion of Successful Self-Regulation*

The opponents' second major argument challenges the necessity of any governmental involvement in the regulation. Industrial players insist that the industry will work out on its own over time, and the government should not

[186] TUROW ET AL., *supra* note 173, at 4.
[187] *Id*.
[188] Frazee et al., *supra* note 81, at 410.
[189] *Id*.
[190] NAT'L RESEARCH COUNCIL, *supra* note 164, at 76.

interfere in the self-regulation and stifle innovation.[191] The general marketing and information reseller industries argue that the regulatory gaps in consumer privacy protections are not that significant[192] and flexible industry self-regulation should be able to adapt to rapid changes in technology and meet consumers' expectations.[193] Relatedly, health IT players claim that any well-meant new set of regulations may "have unintended consequences or lead to a regulatory land grab."[194]

This "let the market play out" stance is generally in line with the U.S. government's long-standing desire to maintain a free market economy and a limited government,[195] and has long prevailed in guiding the U.S.'s privacy policies. For example, the Clinton administration advocated for industrial self-regulation in privacy protection as opposed to governmental regulation.[196] FTC also supported self-regulation as an alternative to "baseline legislation when it comes to privacy protection."[197]

While the role of self-regulation in general consumer privacy regulation is beyond the scope of this Article, this Article argues that at least in terms of regulating mHealth app data, a self-imposed regulatory approach is unlikely to be successful if that self-regulatory mechanism only involves trade associations, third-party organizations, and companies within the industry,[198] and is not backed by any governmental agency.

---

[191] *See* U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 151, at 29–30 (2013) ("industry self-regulation was flexible and could adapt to rapid changes in technology and consumer expectations, whereas legislation and government regulation could be inflexible and quickly become outdated in an era of rapidly evolving technologies; imposing privacy protections by law or regulation, rather than through self-regulatory means, would raise compliance costs for businesses, with these increased costs falling hardest on small operators and start-up companies"); Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461, 463 (2016) (mentioning the argument that businesses are in the best position to decide what are best for them and their consumers and the government should not infringe on the marketplace and burden the data-driven economy); FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESS AND POLICYMAKERS 11 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf (mentioning the argument that the government is impeding the industry's ability to keep up with the rapidly changing marketplace) [https://perma.cc/EB64-7FNV].

[192] U.S. GOV'T ACCOUNTABILITY OFF., *supra* note 151, at 29–30.

[193] *Id.* at 29.

[194] Natalie R. Bilbrough, *The FDA, Congress, and Mobile Health Apps: Lessons from DSHEA and the Regulation of Dietary Supplements*, 74 MD. L. REV. 921, 936 (2015).

[195] Drake, *supra* note 163, at 177.

[196] *Id.*

[197] FED. TRADE COMM'N, *supra* note 191, at 7–13.

[198] *See* Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 J. L. & POL'Y FOR INFO. SOC'Y, 355, 356 (2011).

Self-regulation has succeeded in some sectors such as advertising,[199] but not in the field of consumer privacy protection, let alone the protection of mHealth app data.[200] A paper published by the World Privacy Forum concluded that privacy self-regulation carried out in the past has failed for lack of transparency, credibility, sincerity, staying power, and meaningful enforcement.[201] FTC has similarly noted that "efforts to address privacy through self-regulation have been too slow, and have failed to provide adequate and meaningful protection."[202] HHS also conceded that despite the recent best efforts, no widely adopted voluntary code of conduct has emerged in the area of non-HIPAA health data protection.[203]

Successful self-regulatory initiatives share several features.[204] The following two are critical: (1) sufficient motivation to participate, and (2) effective monitoring and enforcement mechanisms.[205] Unfortunately, the status quo of self-regulation of mHealth app data fails on both counts.

A fundamental problem with self-regulation is that it can only regulate those actors motivated or principled enough to participate.[206] Without governmental interference, mHealth industry players' incentive to take part in self-regulatory programs is quite low because there is no pressure along the industrial chain. Neither customers nor the downstream and upstream players are in a position to require changes. Specifically, the current mHealth app data market suffers two flaws.

---

[199] *See* Maureen K. Ohlhausen, Comm'r, Fed. Trade Comm'n, Address at the Better Business Bureau Self-Regulation Conference—Success in Self-Regulation: Strategies to Bring to the Mobile and Global Era (June 24, 2014), https://www.ftc.gov/system/files/documents/public_statements/410391/140624bbbself-regulation.pdf [https://perma.cc/2BKA-ZQ93].

[200] *See generally* NAT'L TELECOMM. & INFO. ADMIN., U.S. DEP'T OF COMMERCE, *Chapter 1: Theory of Markets and Privacy*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (1997), https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy (providing comprehensive discussions on the roles, limitations and failures of market, government and self-regulation in protecting personal information) [https://perma.cc/6NFR-MUBW].

[201] *See generally* ROBERT GELLMAN & PAM DIXON, WORLD PRIVACY F., MANY FAILURES: A BRIEF HISTORY OF PRIVACY SELF-REGULATION IN THE UNITED STATES (2011), http://www.worldprivacyforum.org/wp-content/uploads/2011/10/WPFselfregulationhistory.pdf (conducting a review of the first wave of privacy self-regulatory efforts in the area of digital privacy protection and finding that the "majority of these industry self-regulatory programs failed," and "many disappeared entirely") [https://perma.cc/9499-UCTM].

[202] John Schinasi, *Practicing Privacy Online: Examining Data Protection Regulations through Google's Global Expansion*, 52 COLUM. J. TRANSNAT'L L. 569, 585 (2014).

[203] U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 98, at 31.

[204] *See* Ohlhausen, *supra* note 199.

[205] *Id.*

[206] A. Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461, 1527–28 (2000).

First, information asymmetry is severe between data collectors, processors and service providers on one side and consumers on the other side. As discussed earlier, information asymmetry prevents customers from making meaningful judgment on data processing and privacy threats, differentiating credible service providers from the inferior, making informed choices about whom they can trust, and eventually acting in their best interest. Thus, data handlers cannot benefit from participating in and complying with any self-regulatory initiative as long as consumers lack the knowledge to seek out those who comply.

Second, in the mHealth app industry, transacting data is much more lucrative than rendering the underlying services where the data comes from. This has shaped the whole data-driven industry. In the absence of external pressure, any "unnecessary" self-imposed limitation will only affect a player's own profitability and its interaction with others within the industry. When a clear conflict of interest arises, and no external pressure exists, low incentive to participate becomes the first hurdle to self-regulation. In the end, profits remain the primary, if not the only, driver of businesses.[207]

Lack of effective monitoring and enforcement actions is the second major obstacle. As noted by many critics, self-regulation lacks accountability and suffers weak oversight and enforcement.[208]

To illustrate, this paragraph examines some recent self-regulation initiatives within the mHealth industry. The first initiative is from the CARIN Alliance, a multi-sector alliance of more than sixty providers, payers, consumers, electronic health record vendors, pharmaceutical companies, consumer platform companies, digital health companies, and consumer advocates.[209] The CARIN Alliance developed a "voluntary code of conduct for entities not covered by HIPAA for handling health care data accessed via application programming interfaces" which requires obtaining "informed, proactive consent from users" and "giving consumers complete access and control over the use of their health care data," and encourages consumer platform companies to "adopt the code as part of their consumer-facing application's registration and onboarding process."[210] The Consumer Electronics Association (CEA) issued its "Guiding Principles on the Privacy and Security of Personal Wellness Data" in October 2015, but adopting these principles is not compulsory for CEA members.[211] Likewise, Xcertia, a self-

[207] Bradyn Fairclough, *Privacy Piracy: The Shortcomings of the United States' Data Privacy Regime and How to Fix It*, 42 J. CORP. L. 461, 464 (2016).
[208] Rubinstein, *supra* note 198, at 356.
[209] *Voluntary Code Established For Handling Health Care Data Not Covered by HIPAA*, 26 GUIDE TO GOOD CLINICAL PRACTICE NEWSL. 10 (2019).
[210] *Id.*
[211] U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 98, at 31.

described "joint mHealth app collaborative effort" between app developers and healthcare organizations, recently finalized its 2019 version of mHealth App Guidelines, including the app privacy guidelines in its first section.[212] The app privacy guidelines provide requirements in several aspects, such as "notice of use and disclosure, data retention, access mechanisms," and compliance with HIPAA, Children's Online Privacy Protection Act (COPPA), and GDPR.[213] In releasing an earlier draft of the 2019 Xcertia guidelines, Xcertia Board Chair Michael Hodgkins noted the "pressing need to establish a framework to evaluate mobile health apps "and said that "Xcertia encourages stakeholders [in the industry] to … support the implementation of these guidelines in the market."[214] By their own terms these standards are only "encouraged."[215] Having standards is good, but standards only have teeth when outliers can be disciplined. Unfortunately, all the existing self-regulation initiatives are toothless.

Judging from the history and the current unsuccessful initiatives, complete self-regulation of privacy standards for mHealth app data is unlikely to be satisfactory. While "big government" intervention may go too far, the government still has a role to play. If there are valid, enforceable government-backed standards, companies that do not intend to undermine consumer privacy can be reassured that they will not face liability. Further, bad actors that undermine consumer privacy may see a legal penalty imposed to restrain from committing any breach of consumer privacy.

B. Comprehensive or Sectoral: A Pragmatic Perspective

From the perspective of governmental regulation, there have been widespread discussions among mHealth industry players, scholars and practitioners over how to regulate non-HIPAA health data. These parties have stressed the importance of reconciling existing data protections with new regulatory changes. Additionally, these parties argue that new regulations must provide sufficient protection while avoiding over-regulation.[216] Kirk Nahra, one of the leading practitioners in the field of privacy and cybersecurity, notes that there may be three options to achieve this balance:

---

[212] XCERTIA, *2019 Board Approved Xcertia Guidelines*, XCERTIA MHEALTH APP GUIDELINES 2019, 3–9 (2019), https://xcertia.org/wp-content/uploads/2019/08/xcertia-guidelines-2019-final.pdf [https://perma.cc/22VW-W5F9].

[213] *Id.*

[214] Eric Wicklund, *Xcertia Releases New mHealth App Guidelines, Adding 3 Categories,* MHEALTHINTELLIGENCE (Feb. 13, 2019), https://mhealthintelligence.com/news/xcertia-releases-new-mhealth-app-guidelines-adding-3-categories [https://perma.cc/A7CE-EVLG].

[215] *Id.*

[216] *See infra* notes 240–42 and accompanying text.

> [1] a specific set of principles applicable only to "non-HIPAA health care data" (with an obvious ambiguity about what "health care data" would mean); [2] a set of principles (through an amendment to the scope of HIPAA or otherwise) that would apply to all health care data; or [3] a broader general privacy law that would apply to all personal data (with or without a carve-out for data currently covered by the HIPAA rules).[217]

An intuitive option would be for Congress to pass a comprehensive consumer data protection law that covers all data, including mHealth app data, regardless of the entities and platforms. This would offer all-inclusive protections, and may integrate all regulatory efforts under a single authority and simplify enforcement actions. Unfortunately, a federal comprehensive solution will not easily succeed due to political stakeholder concerns and potential constitutional challenges.

Therefore, policymakers should take a more pragmatic approach. A more efficient, effective solution for regulating mHealth app data would be to take a sectoral approach based on the federal health privacy exceptionalism policy.[218] Rather than waiting for Congress to pass a comprehensive privacy statute, federal agencies should instead refine the existing health data protection regulatory regime and address the immediate privacy concerns posed by mHealth app data.

1. *All Previous Attempts of Comprehensive Solutions Failed*

Following the implementation of GDPR , members of Congress have introduced a flood of privacy bills, including the Data Care Act,[219] proposed by Senators Brian Schatz, Amy Klobuchar, and Cory Booker,[220] and the Consumer Data Protection Act proposed by Senator Robert Menendez.[221]

---

[217] KIRK NAHRA, WILEY REIN LLP, MOVING TOWARD A NEW HEALTH CARE PRIVACY PARADIGM 4 (2014), (paper submitted to the Office of the National Coordinator for Health Information Technology's Privacy and Security Working Group Virtual Hearing of Dec. 8, 2014), https://www.healthit.gov/sites/default/files/facas/PSWG_Background_Kirk_Nahra_Health_Care_Privacy_Paradigm_2014-12-08.pdf [https://perma.cc/3JKW-AEA9].

[218] *See* Terry, *supra* note 57 at 93–97.

[219] Data Care Act of 2018, S. 3744, 115th Cong. (2018).

[220] Tom Davies, *New Data Protection Bill Could Strengthen Data Privacy Rights of US Consumers,* GDPR: REPORT (Dec. 17, 2018), https://gdpr.report/news/2018/12/17/new-data-protection-bill-could-strengthen-data-privacy-rights-of-us-consumers/ [https://perma.cc/GPF5-WPF3].

[221] Consumer Data Protection Act, S. 2188, 115th Cong. (2018).

While these legislative actions are encouraging, the prospect of passing a comprehensive federal privacy law remains an uphill battle.

Past attempts to pass a federal general privacy protection regime have never succeeded. The BEST Practices Act, the Commercial Privacy Bill of Rights Act, and the Consumer Privacy Protection Act of 2011 were all abandoned by Congress.[222] The Obama administration's 2015 Consumer Privacy Bill of Rights also failed due to criticism from both industry players, who claimed it imposed an undue burden to the business, and privacy advocates, who claimed the privacy protections were inadequate.[223]

2. *Constitutional Challenges*

There are two key constitutional concerns preventing a comprehensive federal privacy statute. First, unlike in other countries (and some states), privacy is not a fundamental right written into the U.S. Constitution. By contrast, the EU has recognized that citizens have a fundamental right to data protection.[224] The right to privacy is recognized in the Charter of Fundamental Rights of the European Union and Treaty on the Functioning of the European Union.[225] Therefore, there was little doubt that adopting comprehensive data protection like GDPR was permissible because it protects a recognized fundamental right.[226] Likewise, some states like California[227] have the right to privacy specifically written into the state's constitution. This in a way explains why "states are leading the way on data privacy" in the United States.[228]

At the federal level, the U.S. Supreme Court has held that privacy is not an enumerated right, but is a protected social value coming from the "penumbras formed by emanations from those guarantees in the Bill of

---

[222] Schinasi, *supra* note 202, at 581.

[223] Paul Bischoff, *What is the Consumer Privacy Bill of Rights and How Has it Evolved?*, COMPARITECH (Nov. 27, 2018), https://www.comparitech.com/blog/vpn-privacy/consumer-privacy-bill-of-rights/ [https://perma.cc/YTB6-XTPC].

[224] Drake, *supra* note 163, at 173.

[225] Minke D. Reijneveld, *Quantified Self, Freedom, and GDPR*, 14 SCRIPTED 285, 288 (2017).

[226] *But see* Bart van der Sloot, *Legal Fundamentalism: Is Data Protection Really a Fundamental Right?*, *in* DATA PROTECTION AND PRIVACY: (IN)VISIBILITIES AND INFRASTRUCTURES 3–5, 8 (Ronald Leenes et al. eds., 2017) (arguing that "data protection" has gradually been disconnected from the right to privacy and should be regarded as a consumer right).

[227] Margaret Betzel, *Privacy Law Developments in California*, 2 I/S: J.L. AND POL'Y 831, 834 (2006).

[228] Andrew Burt, *States Are Leading the Way On Data Privacy*, HILL (Aug. 21, 2018, 10:30 AM), https://thehill.com/opinion/technology/402775-states-are-leading-the-way-on-data-privacy [https://perma.cc/5PRX-7MJT].

Rights."[229] Thus, the Supreme Court has embraced a right to privacy, though the Court has only recognized the right in select areas such as marriage and abortion.[230] As one commentator has noted, this constitutional patchwork parallels the legislative sectoral approach to data privacy.[231]

The second consideration is the tension between freedom of commercial speech under the First Amendment and privacy protection. The Supreme Court's decision in *Sorrell v. IMS Health* is instructive.[232] In *Sorrell*, the Court struck down a Vermont statute restricting the sale and use of pharmaceutical data, holding that the government could not engage in "content" or "viewpoint" discrimination against marketers by prohibiting the commercial use of data while permitting non-commercial use.[233] In that opinion, the Court approved of HIPAA's universal opt-in approach, which specifically regulates healthcare industry players' use of personal data and requires notification to all consumers of how their personal data will be used.[234] The Court's ruling in *Sorrell* supports the sectoral approach, which regulates select sensitive contexts, and rejects approaches where specific harmful uses are carved out from general permissible use of data. This perhaps explains why previous context-specific statutes such as HIPAA and GINA were enacted without facing significant constitutional challenges.

Certainly, the First Amendment is not an absolute bar to a universal data protection regime, but it could be deployed as a powerful argument against such a regime.[235] For instance, Jeff Joseph, President and CEO of the Software & Information Industry Association, recently criticized the California Consumer Privacy Act of 2018 (CCPA), claiming that it lacks a compelling public purpose and engages in content-based discrimination.[236] He further argued that any federal-level privacy legislation had to "be structured to accomplish their important purpose in a way that is the least restrictive of

---

[229] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).
[230] Michael C. James, *A Comparative Analysis of the Right to Privacy in the United States, Canada and Europe*, 29 CONN. J. INT'L L. 257, 268 (2013).
[231] *Id.* at 270.
[232] Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).
[233] *Id.* at 565.
[234] Katie Booth, *The All-or-Nothing Approach to Data Privacy:* Sorrell v. IMS Health*,* Citizens United*, and the Future of Online Data Privacy Legislation*, HARV. J. OF L. & TECH.: JOLT DIGEST (Vivian Tao ed., Aug. 17, 2011), https://jolt.law.harvard.edu/digest/the-all-or-nothing-approach-to-data-privacy-sorrell-v-ims-health-citizens-united-and-the-future-of-online-data-privacy-legislation [https://perma.cc/5KST-KYJA].
[235] *See* Christopher Mohr, *Data is Speech: The Constitution Has a Role in Informational Privacy II*, SIIA (Oct. 11, 2018), http://www.siia.net/blog/index/Post/76979/Data-is-Speech-The-Constitution-Has-a-Role-in-Informational-Privacy-II [https://perma.cc/73ZP-LEXL].
[236] Donald Gilliland, *We Need a National Privacy Law That Respects the First Amendment,* HILL (Mar. 13, 2019, 1:30 PM), https://thehill.com/opinion/technology/433621-we-need-a-national-privacy-law-that-respects-the-first-amendment [https://perma.cc/S26P-XLQ9].

speech."[237] Legislators need to address these potential arguments and polish the wording of any future privacy statute; they must differentiate between "permissible" and "harmful" uses of data and strike a careful balance between commercial needs and data protection.[238]

3. *Stakeholder Concerns*

The reactions of certain classes of stakeholders will have an impact on whether a given comprehensive privacy measure will succeed. In response to any comprehensive privacy bill, industry players will likely to be the first to fight. According to Karsten Weide, Media and Entertainment Program Vice President at International Data Corporation (IDC), "growing demand would cause data vendor sales to more than triple to $10.1 billion by 2022, compared with $3.1 billion in 2017."[239] If any general privacy legislation is adopted, data vendors stand to suffer, and the survival of the broader data-selling industry would be at risk. As one commentator said: "prepare for a new privacy lobbying battle."[240]

Beyond industrial stakeholders, the federal government has consistently been reluctant to either make significant structural changes to the existing sectoral framework or to pass a comprehensive privacy law. For example, while proposing a comprehensive consumer privacy bill to Congress, the Obama administration limited the proposal to "commercial sectors that are not subject to existing federal data privacy laws."[241] FTC also cautioned that overlapping or duplicative requirements should be avoided and suggested that a general data protection law should not apply to the entities that are subject to sector-specific laws like HIPAA.[242] The Trump administration said that the sectoral approach provided strong, focused

---

[237] *Id.*

[238] *See generally* Marsha Cope Huie, Stephen F. Laribee & Stephen D. Hogan, *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 470 (2002) (providing a historical review and discussions about conflict between freedom of commercial speech and privacy).

[239] Aliya Ram & Madhumita Murgia, *Data Brokers: Regulators Try To Rein In The "Privacy Deathstars,"* FIN. TIMES (Jan. 7, 2019), https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521 [https://perma.cc/2ASM-SA5G].

[240] David Meyer, *In the Wake of GDPR, Will the U.S. Embrace Data Privacy?*, FORTUNE (Nov. 29, 2018), http://fortune.com/2018/11/29/federal-data-privacy-law/ [https://perma.cc/5XMT-7CQ7].

[241] Terry, *supra* note 57, at 96.

[242] *Id.* at 97.

protections that should be maintained, and called for actions addressing consumer privacy in areas that are not currently covered by sectoral laws.[243]

Even if passed, comprehensive legislation would most likely only address baseline privacy issues and leave sector-specific details to industry regulators. In the case of health data, comprehensive legislation might simply carve out HIPAA-covered data. In that case, it would not be a problem to first fill the identified gaps of the current sectoral regulations.

4. *Health Privacy Exceptionalism*

A sectoral approach would not be a mere second-best solution. The policy of health privacy exceptionalism, as frequently discussed by Nicolas P. Terry,[244] should be continued for regulation of mHealth app data. If a policy of health privacy exceptionalism is extended to mHealth app data, a sectoral approach would be justified. This Section argues that compared with other consumer data, which can to some extent give way to commercial innovation, mHealth app data warrants the government's exceptional regulatory attention, and should be covered by the long-standing health privacy exceptionalism.

First, as discussed in Part I, mHealth apps are the main, if not the largest, source of non-HIPAA health data. Some highly sensitive mHealth app data can pose significant harms to data subjects if misused in combination with Big Data analytics, just like traditional HIPAA-regulated health data.

Second, existing statutes cannot fully mitigate the harms posed by misuse of mHealth app. This further justifies the necessity of imposing robust *ex ante* regulations for mHealth app data and the continuance of health privacy exceptionalism.

For example, there are already anti-discrimination laws that cover the use of health data, but they do not cover most mHealth app data. The Americans with Disabilities Act (ADA) is supposed to prevent disability-based discrimination, but it does not prohibit predictions of future disability on the basis of data regarding things like health habits, stress level, and exposure to environmental pollutants.[245] GINA better protects consumers by prohibiting discrimination based on genetic information and gene-based inference and suspicion, but the law only covers genetic information and

---

[243] STEPHEN MULLIGAN ET AL., CONG. RESEARCH SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW, 52 (2019) https://crsreports.congress.gov/product/pdf/R/R45631 [https://perma.cc/2GF6-7Z7P]; *see also* Developing the Administration's Approach to Consumer Privacy, 83 Fed. Reg. 48,600, 48,601 (Sept. 26, 2018), https://www.federalregister.gov/documents/2018/09/26/2018-20941/developing-the-administrations-approach-to-consumer-privacy [https://perma.cc/SKF3-PR5Z].

[244] *See* Terry, *supra* note 57.

[245] Hoffman, *supra* note 72, at 93.

applies only to health insurers and employers.[246] Both statutes fail to completely prevent discriminatory use of mHealth app data because mHealth app data may involve more kinds of health data (inherently or context-based, descriptive or predictive), more areas of health data (e.g., genetic information, illness, chronic conditions), and more actors (e.g., marketers, credit-card companies).

Actually, the government has adopted this exceptionalism approach to deal with other similarly sensitive data, when a stringent, general regulation is not advisable. For instance, in response to the pressing needs of regulating the problematic gathering and use of children's personal data as found in a 1998 FTC survey,[247] FTC designed protections for children's online privacy and passed COPPA to govern the collection and use of personal information from minors.[248] In 2013, COPPA was revised to enhance the regulatory protection by including an expanded definition of "personal information," and the definition of "commercial website operator."[249] The exceptionalism mindset behind COPPA is the same: Although commercial innovation and development are valid considerations and should not be unnecessarily impeded, the social costs and potential risks associated with misuse of certain especially sensitive data are too high to tolerate.

To conclude, it seems prudent, at least at the outset, for the government to adopt a conservative approach to the regulation of mHealth app data and determine whether a lighter touch is possible in the future, when the industry is accustomed to, and customers are well educated on, good privacy practices. Granted, mHealth app data may meanwhile include some less sensitive data that does not necessarily deserve exceptional protections. However, that is something left for regulators to consider when designing the regulatory framework, not a pretext to deny robust regulations for mHealth app data altogether.

C. A Two-Prong Solution

Following the sectoral approach, this Section proposes a two-prong solution based on the existing HIPAA-FTC framework to grant mHealth app

---

[246] *Id.* at 94.

[247] FED. TRADE COMM'N, IMPLEMENTING THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT–A REPORT TO CONGRESS 3 (2007), https://www.ftc.gov/sites/default/files/documents/reports/implementing-childrens-online-privacy-protection-act-federal-trade-commission-report-congress/07coppa_report_to_congress.pdf [https://perma.cc/SHN3-8BCM].

[248] MULLIGAN ET AL., *supra* note 243, at 52.

[249] Christina Scelsi, *Care and Feeding of Privacy Policies and Keeping the Big Data Monster at Bay: Legal Concerns in Healthcare in the Age of the Internet of Things*, 39 NOVA L. REV. 391, 411 (2015).

data different levels of protection according to their risk levels. Such a balanced proposal can capture all mHealth app data, but avoid over-regulation in the meantime.

Under this proposal, mHealth app data is classified into two defined categories: "mHealth data" and "mHealth consumer data." mHealth data is mHealth app data qualifying as health data under the two-step definition discussed in Part I, and mHealth consumer data is mHealth app data other than mHealth data. mHealth data, the related apps, and the entities handling them will be governed by HIPAA after its proper expansion. mHealth consumer data, the related apps, and the entities handling them will be regulated through an FTC-led co-regulation mechanism embedded with principles such as data minimization, purpose specification, and contextual consistency.

1. *First Things First: Categorizing mHealth App Data*

Before discussing the proposed regulatory approach, it is necessary to determine how mHealth app data should be categorized for regulation purposes.

a. Different Approaches in Defining Regulated Health Data

(1) Regulated Health Data under HIPAA

The current HIPAA Rules regulate any information, whether oral or recorded in any form or medium, that is created or received by a covered entity or a business associate and relates to (a) the past, present, or future physical or mental health or condition of an individual, (b) the provision of health care to an individual, or (c) the past, present, or future payment for the provision of health care to an individual.[250] "Health care" means "care, services or supplies related to the health of an individual," including (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body, and (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.[251] By such a broad definition, regardless of the nature of data, all data identifiable to an individual collected or processed by a HIPAA-covered entity is PHI governed by HIPAA.[252] As discussed earlier, it is the type of data holders (rather than the sensitivity of the data) that is the dispositive factor in determining whether certain health

[250] U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 98, at 28.
[251] 45 C.F.R. § 160.103 (2019).
[252] U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 98, at 3.

data will be regulated by HIPAA. In that sense, HIPAA is both over-inclusive and under-inclusive.

(2) Regulated Health Data under GDPR

By contrast, GDPR regulates "data concerning health," and defines data concerning health as "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status."[253] This definition is further clarified by Recital 35 of GDPR by providing examples of what the regulators intend to cover.[254] Recital 35 states that:

> Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.[255]

Regardless of the sources and custodians, GDPR is more focused on the inherent characteristics of the data at issue than HIPAA, but GDPR's definition is over-inclusive and may be unmanageable.

[253] Mantovani et al., *supra* note 169, at 90.
[254] *Id.*
[255] Regulation (EU) 2016/679 2016 O.J (L 119/6) (General Data Protection Regulation).

(3) Regulated Health Data under EU mHealth Code

The draft Privacy Code of Conduct on Mobile Health (mHealth) Apps facilitated by the European Commission[256] (the EU mHealth Code) and its former supervising body the Article 29 Working Party have provided a context-based, fact-specific approach in categorizing health data.[257] The draft EU mHealth Code states that "the context of processing, and particularly the purpose for which the app is made available or whether the data is made available through the app to a member of the medical community, is also relevant to determine whether data should be qualified as data concerning health."[258]

The Article 29 Working Party further contended that to determine whether certain data is health data, not only the type of the data, but also the intended use of the data and its combination with other datasets should be considered; specifically, personal data is health data when (1) the data is inherently or clearly medical data; (2) the data is raw sensor data that can be used in itself or in combination with other data to draw a health-related conclusion; or (3) conclusions are drawn about a person's health status or health risk.[259]

The EU mHealth Code's approach generally fits the two-step definition discussed in Part I, but without a workable tool, this approach could be open-ended and unmanageable, especially for the context test in the second step.

b. Proposed Approach in Categorizing Regulated Data

To avoid over-inclusion or under-inclusion and to provide a workable approach, this Section suggests that mHealth app data be categorized by a combination of FDA's classification of mHealth apps and the two-step definition of health data discussed in Part I. Specifically, FDA's classification of mHealth apps has provided a practical tool in applying the test of health-

[256] Press Release, European Commission, Code of Conduct on Privacy for mHealth Apps Has Been Finalised (Jun. 7, 2016), https://ec.europa.eu/digital-single-market/en/news/code-conduct-privacy-mhealth-apps-has-been-finalised (stating that the Privacy Code of Conduct on mobile health (mHealth) apps aims to promote trust among users of mHealth apps and will provide a competitive advantage for those who sign up to it in the future) [https://perma.cc/886M-EAGD].

[257] Mantovani et al., *supra* note169, at 90–91.

[258] EUROPEAN COMMISSION, DRAFT CODE OF CONDUCT ON PRIVACY FOR MOBILE HEALTH APPLICATIONS 2 (2016), http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=16125 (click the "Code" hyperlink in the press release text) [https://perma.cc/3R85-X33P].

[259] Mantovani et al., *supra* note 169, at 90–91.

related context in the second step of the definition. This combined approach creates two categories of data:

First, "mHealth data" refers to data generated by the first and second categories of mHealth apps under FDA's classification, namely those mHealth apps qualifying as devices under the FDCA. As discussed previously, such data is either inherently medically meaningful under the first step of the new definition or collected and used in a medical context under the second step of the new definition.

Second, "mHealth consumer data" refers to data generated by the third category of mHealth apps. Such data usually (1) does not by itself point to any specific disease or condition, and (2) does not incur any medical context or proclaim any medical-related purpose. The caveat is that if any data generated by the third category of mHealth apps is inherently medically meaningful, it should, according to the first step of the new definition, always be considered mHealth data. For example, if one app is designed to check your ancestry, not to identify diseases, the genetic data so collected and generated should still be considered mHealth data because it is inherently health-related, although the data is used outside a medical context.

2. *Expanding HIPAA to Cover mHealth Data*

HIPAA should expand its reach to include mHealth data and enhance the data minimization requirement to address the concern of excessive data collection. Because mHealth data is sensitive data generated in non-HIPAA health-related settings it should receive the same treatment as HIPAA-covered health data presently. The current HIPAA exceptions, such as free use for public health research purposes, should also apply to mHealth data. The proposed expansion has two aspects.

First, HIPAA should change its covered entity paradigm and regulate all entities and mHealth apps that collect, use, and process mHealth data. Although mHealth data is collected and processed outside the traditional medical setting, the nature of this data is similar to data held by the HIPAA-defined covered entities and business associates in terms of sensitivity and risks.

In response to this call to expand HIPAA, HHS stated that the HIPAA Rules work only for healthcare providers and insurers, and a simple extension of HPAA may not be practical.[260] This argument might not be convincing.

The current HIPAA Rules do not only apply to healthcare providers and insurers, but also their business associates—including any non-medical entity providing, among other things, legal, accounting, and IT services. In particular, some mHealth data collected on behalf of health providers by apps in the capacity of business associates have already been regulated under HIPAA. For instance, PHR vendors—who qualify as business associates—may provide online accounts linked to wearable health and fitness devices to collect PHI on behalf of covered entities so that health care providers can then advise their patients about their health based on the data collected.[261] The activity of PHR vendors is comparable to that of developers of consumer-facing mHealth apps, except they are engaged by covered entities and qualify as business associates.

Some provisions of the HIPAA Rules may need to be refined to fit mHealth data collectors. For example, the current rules rely on Institutional Review Boards (IRB) and privacy boards that are appropriate for large institutions and require significant resources and expertise.[262] These boards may not be compatible with or appropriate for consumer-generated mHealth data because of the overhead and relatively lower professional standards involved, but they are only one part of the HIPAA Rules. Most of the HIPAA Rules are privacy-related requirements for general use which could be adopted to govern smaller developers. With necessary refinements to address these resource issues the expansion of HIPAA to cover these developers should be practical.

Second, HIPAA should expand its regulatory scope by enhancing data subjects' control over their health data, especially upstream protection regarding data collection. This would be a necessary accommodation because of the combination of mHealth technology and Big Data analytics. As discussed earlier, because the HIPAA Rules were only contemplating the traditional clinical setting at their enactment, disclosure of personal information by data subjects was assumed. However, the current technologies have incentivized excessive data collection and posed pressing privacy

---

[260] NAT'L COMM. VITAL & HEALTH. STATISTICS, U.S. DEP'T HEALTH & HUMAN SERVS., HEALTH INFORMATION PRIVACY BEYOND HIPAA: A 2018 ENVIRONMENTAL SCAN OF MAJOR TRENDS AND CHALLENGES 51 (2017), https://ncvhs.hhs.gov/wp-content/uploads/2018/05/NCVHS-Beyond-HIPAA_Report-Final-02-08-18.pdf ("The same rules may not work in the same way for other health data processors so that any simple extension of HIPAA may not be practical.") [https://perma.cc/VQ7H-DMAN].

[261] WU, *supra* note 101, at 31.

[262] 45 C.F.R. § 164.512(i) (2019).

concerns. After examining GDPR, CCPA, and FIPPS, the following principles should be added to strengthen HIPAA's upstream protections.

(1) *Data minimization for data collection*. Currently HIPAA imposes a minimum necessary requirement to the downstream (post-collection) area of health data. Specifically, the minimum necessary standard requires covered entities to allow access to and disclosure of PHI on a need-to-know basis.[263] A covered entity then must set up and implement mechanisms for role-based access and use of PHI among its members of the workforce.[264] Such a minimum necessary standard is now equally important at the data collection stage if mHealth data is to be covered. The rationale is that only data necessary to implement mHealth apps' functions for the stated purposes should be collected, and relevant policies and procedures should similarly be developed to implement this standard.

To be clear, the proposed upstream limitations are not to unreasonably limit data collection and frustrate mHealth apps' purposes, but to ensure that data collection takes place only to the extent necessary and in a transparent way. Because of the lax regulatory environment, current extensive data collection practices may be the core part of the business model and the main profit source for many mHealth apps. Had there been upstream limitations, these apps would perhaps never have been created. Some may argue that if upstream limitations were imposed, there would undoubtedly be a loss to these businesses. However, that is exactly one of the issues that should be tackled by data protection regulations: mHealth app data is supposed to fulfill meaningful health-related functions in exchange for reasonable returns, rather than profiting from mining, exploiting, and selling data against data subjects' interests. If an mHealth app's primary purpose is to take advantage of consumers' privacy, it makes sense to have the statutory upstream limitations to screen it out. A pure financial loss argument from commercial actors should not defeat the necessity of adding upstream limitations into HIPAA to prevent unreasonable collection, mining, and exploitation of health data.

(2) *Right to deletion*. The right to deletion is the other side of the coin of data minimization. Similar rights have been embraced by GDPR and CCPA. For example, GDPR gives a data subject the right of erasure of his or her personal data without undue delay when, among other criteria, (i) the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed; (ii) the data subject objects to processing and there are no overriding legitimate grounds for the processing; (iii) the personal data has been unlawfully processed; or (iv) the personal data has to

---

[263] U.S. DEP'T OF HEALTH & HUMAN SERVS., OCR HIPAA PRIVACY, MINIMUM NECESSARY (2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/minimumnecessary.pdf [https://perma.cc/YG6E-Y2EE].

[264] U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 106, at 10.

be erased for the data subject to be in compliance with a legal obligation.[265] Of course, such a right is not unlimited. GDPR does have exceptions to the right to erasure that address situations in which retention is desirable for, among others, public health or scientific archiving reasons.[266] The right to deletion set forth in CCPA seems to be more business-friendly because it expressly provides that the right to deletion is not exercisable if the data in question is needed for completing transactions, maintaining business relationships, performing contracts, and solely for reasonable internal use.[267]

HIPAA takes the opposite approach. As part of the documentation requirements, covered entities are required to retain the data for "6 years from the date of its creation or the date when it last was in effect, whichever is later."[268] This Article suggests that HIPAA should similarly grant data subjects a right to request deletion of their health data if such data is no longer relevant or necessary, subject to reasonable exceptions such as use for public health research or for business necessity.

Although the public health exception for the right to deletion could easily follow the existing HIPAA standards, the applicability of the reasonable business necessity exception would invite more debate, because it must be crafted to support legitimate business functions without permitting more invasive data mining. This Article does not attempt to go into the details regarding the possible interpretations of this exception but proposes two premises on which this exception should be based.

First, the business necessity of the data collection should be made clear to data subjects so that they are able to make an informed choice about participation before the data is collected. As an example, consider a gene testing app that presents two options to users. One option is a one-off test to check ancestry or disease risks; the other is a five-year gene research program in exchange for a discount. If a user only opts in the one-off test, there is no basis for the app to claim business necessity even if the app's primary business model is based on data aggregation. This lack of business necessity is an incentive for users to opt for the one-off test—just as much as the discount is an incentive for them to opt for the five-year program. This information should be presented to users before they select an option.

Second, reliable de-identification measures should be in place if an app invokes the business necessity exception to retain users' data so that the

---

[265] Tovino, *supra* note 99, at 990–91.
[266] *Id.* at 991.
[267] David Kessler & Anna Rudawski, *CCPA Extends "Right to Deletion" to California Residents*, NORTON ROSE FULBRIGHT BLOG NETWORK: DATA PROTECTION REPORT (Sept. 27, 2018), https://www.dataprotectionreport.com/2018/09/ccpa-extends-right-to-deletion-to-california-residents [https://perma.cc/RSM6-FQVF].
[268] 45 C.F.R. § 164.316 (2019).

exposures to data-related harms can be reduced to a minimal level. That is, if the data invokes the exception and does not delete the data, it should at least be de-identified with robust technologies to protect against re-identification.

3. *FTC-led Co-regulation: Taking It a Step Further*

For regulation of mHealth consumer data, this Article suggests that FTC take a step forward to turn self-regulation into co-regulation. As a collaborative process, co-regulation is a middle ground between complete self-regulation and strict agency regulation.

a. Success Stories of Co-regulation

Co-regulation is not a new creature, but a verified, effective methodology. Before the passage of GDPR, the EU used a co-regulatory approach to protect privacy. The typical process went as follows: after a member state passed a comprehensive data protection statute, sectoral representatives would be invited to draft a code of conduct for different sectors detailing the data protection requirements.[269] Once approved by the regulator, the drafted code of conduct would take on the force of law, and data custodians within that sector could be punished for noncompliance.[270]

Currently, the EU intends to continue this approach to regulate mHealth apps.[271] The European Commission is now facilitating the passage of the EU mHealth Code.[272] If no more comments are received, the current draft will be approved by the European Data Protection Board and be granted general validity across the EU.[273] An app provider intending to obey this code of conduct may apply for a trust mark for its app and, once approved label its app with the trust mark.[274] Accordingly, adherence to an approved code of conduct would be "an element to demonstrate compliance" with data protection requirements.[275]

Co-regulation is not new in the United States either. In fact, the White House acknowledged the merits of such a collaborative, multi-stakeholder

---

[269] Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation*, 34 SEATTLE U. L. REV. 439, 442 (2011).
[270] *Id.*
[271] Press Release, European Commission, Privacy Code of Conduct on Mobile Health Apps (Dec. 10, 2018), https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps [https://perma.cc/XMQ6-Y72A].
[272] *Id.*
[273] *Id*.
[274] EUROPEAN COMMISSION, *supra* note 258, at 74.
[275] Mantovani et al., *supra* note 169, at 73.

process in a 2012 report.[276] The report stated that the federal government intended to convene discussions among stakeholders to develop industry-specific codes of conduct to protect privacy; stakeholders include companies, consumers, privacy advocates, international partners, state attorneys general, federal criminal and civil law enforcement representatives, and academics.[277]

Federal agencies already have some success stories of co-regulation, although the legal criteria and distribution of responsibilities are different from the EU practice. According to the EU practice, industry-made codes of conduct would be recognized as having direct applicability across the EU, but the U.S. practice is more focused on utilizing the expertise of the industry and relevant associations to come up with and incorporate professional standards. The FDA-USP model is a typical example. United States Pharmacopeia (USP) is a non-profit organization relying on its convention member organizations and their delegates to discuss important industry issues and to carry out critical governance activities. Its members include academic institutions, health practitioners, scientific associations, consumer organizations, manufacturer and trade associations, government bodies, and non-governmental standards-setting and conformity assessment bodies.[278] USP developed and published standards for drug substances, drug products, excipients, and dietary supplements in the United States Pharmacopeia-National Formulary, and these standards were officially recognized through the Federal Food and Drug Act of 1906.[279] Today, USP's compendial standards remain connected to FDA provisions and other consumer protection laws and regulations.[280] Although USP does not have its own enforcement power, FDA enforces any breach of USP standards or provisions.[281]

In the field of health IT, the Office of the National Coordinator for Health Information Technology (ONC) has been successfully operating a voluntary certification program of health IT since 2010.[282] This program is a

---

[276] WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 2 (2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf [https://perma.cc/LZ4V-3MHS].

[277] *Id.*

[278] U.S. Pharmacopeia, *Convention Membership*, USP.ORG, http://www.usp.org/about/convention-membership (last visited Dec. 21, 2019) [https://perma.cc/38UJ-X94B].

[279] Sarah Jean Kilker, *Effectiveness of Federal Regulation of Mobile Medical Applications*, 93 WASH. U. L. REV. 1341, 1353 (2016).

[280] U.S. Pharmacopeia, *USP and the FDA Working Together to Protect Public Health,* USP.ORG, http://www.usp.org/about/public-policy/usp-fda-roles (last visited Dec. 21, 2019) [https://perma.cc/5ZUC-8CNW].

[281] Kilker, *supra* note 279.

[282] *See generally* OFFICE NAT'L COORDINATOR FOR HEALTH INFO. TECH., U.S. DEP'T HEALTH & HUMAN SERVS., HEALTH IT CERTIFICATION PROGRAM

quasi-co-regulation mechanism. First, ONC establishes the underlying program requirements and certification criteria for certified health IT, taking into consideration input from within the federal government, as well as from public and private stakeholders.[283] Second, ONC collaborates with third-party organizations to perform functions such as conformance testing, certification issuing, and surveillance, and health IT developers apply for certification on a voluntary basis.[284] Meanwhile, ONC maintains a complementary power of direct review to promote health IT developers' accountability for performance, reliability, and safety of health IT.[285]

b. Proposed Co-Regulation Approach for mHealth Consumer Data

The co-regulation approach for mHealth consumer data proposed by this Article is a similar collaborative process. Specifically, the approach consists of the following:

(1) *Development of Code of Conduct*. First, a trusted public-private entity representing various interests—including regulators, app developers, app platforms, privacy advocates, end users, and industry experts—should be created or, if feasible, selected from among the existing third-party organizations. The public-private entity would develop a code of conduct for mHealth app data protection through multi-stakeholder negotiations.

(2) *FTC Approval of Code of Conduct.* Second, FTC would review, comment on, and finally approve a code of conduct to ensure that FIPPS principles, FTC's principles summarized from its own enforcement experience, and other widely acknowledged privacy protection practices (such as enhanced notice and express consent for sensitive use, as stated in GDPR) are in place.

(3) *Voluntary Opt-in for Trust Mark.* Third, mHealth app developers intending to adhere to the FTC-approved code of conduct would submit a privacy impact assessment to the public-private entity for review of possible privacy risks and recommendations of any appropriate mitigating measures. If the privacy impact assessment is passed, applicants would be qualified to voluntarily apply for a trust mark from the public-private entity by submitting a declaration of adherence, which would be registered with FTC for record and publication. If a trust mark is granted, the app developers would be entitled

---

OVERVIEW (2019), https://www.healthit.gov/sites/default/files/PUBLICHealthITCertificationProgramOverview.pdf (providing an overview of the Health IT Certification Program, including the program participants, program structure, surveillance of certified health IT, and ONC's direct review of certified health IT) [https://perma.cc/T6SC-HFGT].

[283] *Id.* at 2.

[284] *Id.* at 1.

[285] *Id.* at 4.

to label their apps with such marks. End users, as well as healthcare providers who recommend mHealth apps to their patients, would be educated that mHealth apps with trust marks are government-endorsed and trustworthy.

(4) *FTC's Section 5 Enforcement.* Finally, if an adhering app developer is found to be in violation of the code of conduct as a result of a random check, a verified consumer's complaint, or otherwise, FTC would exercise its existing enforcement power under the deceptiveness prong of Section 5 of the FTC Act and rescind such developer's trust marks. The results of such enforcement would be announced to the public.

As long as appropriately structured, this co-regulation approach would have several advantages over agency regulation and self-regulation. Unlike traditional agency regulation, this mechanism would delegate operational tasks such as developing industry-specific codes of conduct, assessing privacy impacts, and issuing trust marks to a specific public-private entity so that rulemaking and monitoring can be conducted in a relatively neutral, professional, efficient, and customized way.

In the meantime, this government-sponsored initiative can also address the two concerns posed by complete self-regulation discussed earlier: One is that self-regulation lacks sufficient incentive for the players to obey, and the other is that no enforcement is guaranteed.

With respect to the first concern, under this framework, external factors would provide adequate incentive for app providers to adhere to their industry's code of conduct for fear of losing consumers' trust and market competitiveness. Current self-regulation efforts by purely private entities are scattered and without credibility, while this co-regulation approach is centralized, well-structured, and authoritative. The granted trust mark acts as a simple, straightforward, and credible identifier of trustworthy mHealth apps, and places pressures on industry players from the outside. Some may doubt the significance of such a trust mark, but experience has shown that it can calibrate information asymmetry and effectively direct consumers' choices. For example, privacy seals, similar to trust marks, issued by TRUSTe in the 1990s have been a key driver for websites to formulate privacy policies and conform to basic privacy norms.[286] An indication of the government's endorsement would only reinforce such function.

As to the second concern, adhering app providers would clearly trigger FTC's existing Section 5 power if opting-in app providers breach consumers' privacy and violate its own declaration of adherence as a result. No additional interpretation or standards would be needed in this respect.

[286] Solove & Hartzog, *supra* note 93, at 593.

Proponents of co-regulation see it as "the best of both worlds."[287] Although it may be a stretch to consider co-regulation a perfect solution, it does present a good combination of strengths of the different players, with industries as experts and the government as an enforcer,[288] and should at least be an effective stopgap measure to fill the current regulatory gaps.[289]

V. CONCLUSION

Extensive use of mHealth apps and Big Data analytics have blurred the line between health data and other consumer data and have allowed entities outside the traditional healthcare ecosystem to collect, hold, transmit, and process health data. New privacy concerns arising from mHealth technological developments have posed new challenges to the current U.S. regulatory framework for health data protection.

HIPAA does not regulate most mHealth app data. FDA is hands-off to data protection. FTC stands to regulate consumer data in general, including mHealth app data, but is unfortunately constrained by an absence of clear standards and by limited police power. These regulatory gaps need to be addressed.

It seems that Congress is now considering passing a comprehensive consumer data protection statute, given the increased attention to privacy issues and enhanced enforcement by peer nations. However, whether such an effort will come to fruition remains an open question due to some debatable constitutional concerns and political considerations.

This Article argues that, before any general consumer privacy law is passed, a more effective, practical solution would be to refine the current framework to regulate mHealth app data. It proposes a single two-prong solution to provide different levels of protection to different categories of mHealth app data.

FDA's functionality-based typology of mHealth apps, in combination with the two-step definition of health data in the era of Big Data proposed by this Article, would help determine the categorization of sensitive mHealth data

---

[287] *See* Hirsch, *supra* note 269, at 441.

[288] *Id.*

[289] It is also suggested that under this two-prong regulatory framework, FTC, HHS, and FDA, develop a cross-agency tool to assist mHealth app developers assess the kinds of mHealth app data they collect (mHealth data or mHealth consumer data) and determine whether the developers should comply with the HIPAA Rules, turn to the FTC co-regulation regime for trust marks, or do both, just as these agencies did with the previously-developed Mobile Health Apps Interactive Tool. *See* FED. TRADE COMM'N, MOBILE HEALTH APPS INTERACTIVE TOOL, https://www.ftc.gov/tips-advice/business-center/guidance/mobile-health-apps-interactive-tool [https://perma.cc/XV5N-FFJV].

versus less sensitive mHealth consumer data. mHealth data is health data and would be covered by the expanded HIPAA.

mHealth consumer data is less sensitive than mHealth data but overall more health-related and more likely to become health data than other consumer data due to the context set by the mHealth apps in question. As a result, such data would be governed by a co-regulation regime endorsed by FTC and stricter than the current regulation-free situation. This co-regulation approach would include industry-specific codes of conduct representing interests of different stakeholders and would introduce a trust mark mechanism to motivate industry players and address information asymmetry issues among consumers. As a middle ground between complete self-regulation and traditional agency regulation, this co-regulation regime properly combines the expertise of industry players with the enforcement power of the relevant government agency.