Hastings Science and Technology Law Journal

Volume 13
Number 1 *Winter 2022*

Article 4

Winter 2022

Privacy in Wearables: Innovation, Regulation, or Neither

Kenny Gutierrez

Privacy in Wearables: Innovation, Regulation, or Neither

KENNY GUTIERREZ*

TABLE OF CONTENTS

* Kenny Gutierrez is a Bridge Fellow at the Electronic Frontier Foundation.

Background

The digital age is set to experience the production of more than 163 zettabytes (i.e., one-trillion gigabytes) of data per year by 2025, much of which will be consumer-specific.[1] Over the past decade, downloads of mobile health (mHealth) apps and wearables have been on the rise year after year.[2] mHealth apps include both medical apps, and health and fitness apps.[3] mHealth apps run on phones and wearables. Consequently, since wearables gather health information on their users, they will increasingly become a source of data creation.

Technology firms increasingly want a bigger share of the more than three trillion dollars spent annually on health care in the United States.[4] 65% of smartphone users have an mHealth app on their phone.[5] The wearables market is expected to experience significant growth.[6] The combination of mHealth apps and wearables may support consumers in their pursuit of

1. Andrew Cave, *What Will We Do When The World's Data Hit's 163 Zettabytes in 2025?*, FORBES, https://www.forbes.com/sites/andrewcave/2017/04/13/what-will-we-do-when-the-worlds-data-hits-163-zettabytes-in-2025/ (last visited Mar. 1, 2020).

2. Aaron Smith, *Record shares of Americans now Own smartphones, have home broadband*, PEW RSCH. CTR. (Jan. 12, 2017), https://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/; *see also* Lionel Sujay Vailshery, Statistical Report, *Number of connected wearable devices worldwide by region from 2015 to 2022*, STATISTA (Jan. 22, 2021), https://www.statista.com/statistics/490231/wearable-devices-worldwide-by-region/.

3. *mHealth Market Size, Share & Trends Analysis Report By Component (Wearables, mHealth Apps), By Service (Monitoring, Diagnosis), By Participant (Mobile Operators, Device Vendors), By Region, And Segment Forecasts, 2020 – 2027*, GRAND VIEW RSCH. (Feb. 2020), https://www.grandviewresearch.com/industry-analysis/mhealth-market (last visited Apr. 19, 2020).

4. Natasha Singer, *How Big Tech Is Going After Your Health Care*, N.Y. TIMES (Dec. 26, 2017), https://www.nytimes.com/2017/12/26/technology/big-tech-health-care.html (last visited Mar. 1, 2020).

5. Mindsea Team, *28 Mobile App Statistics To Know In 2021*, MINDSEA, https://mindsea.com/app-stats/ (last visited Apr. 14, 2020).

6. *Wearable Devices Market 2019 Size, Industry Share, Approaches and Forecast By 2024 - Market Research Engine*, MARKETWATCH, https://www.marketwatch.com/press-release/wearable-devices-market-2019-size-industry-share-approaches-and-forecast-by-2024—-market-research-engine-2019-09-24 (last visited Mar. 18, 2020) (In 2019, the wearables market was valued at $67 billion; and, the mHealth market was valued at $40.7 billion); INT'L DATA CORP., *Worldwide Wearables Market Braces for Short-Term Impact Before Recovery in 2020, According to IDC*, INT'L DATA CORP. (Mar. 16. 2020), https://www.idc.com/getdoc.jsp?containerId=prUS46138520 (The global wearables market is expected to grow 9.4% in 2020, reaching 368.2 million shipments); Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. OF THE MO. BAR 76, 77 (2018) (This is up from 30.9 million shipments in 2015).

health goals, such as weight management,[7] stress management,[8] smoking cessation,[9] self-management of health conditions,[10] and, more recently, social-distancing measures in light of COVID-19.[11] Wearables with sensors can collect bodily metrics such as glucose levels, blood pressure, blood oxygen levels, sleep patterns, and blood coagulation rates.[12] In all, these broad sets of data are highly attractive to data brokers, technology firms, advertising firms, and the medical community.

Precision medicine is the promise of better treatment outcomes when consumers use apps that create a precise record of their symptoms and behaviors. In 2015, President Obama announced the launch of the Precision Medicine Initiative.[13] Until recently, medical treatments were designed for the "average patient" – a "one-size-fits-all" approach. "Precision medicine . . . is an innovative approach that takes into account individual differences in people's genes, environments, and lifestyles."[14] Wearables gather information about the user's lifestyle to create a data set to develop precision medicine.

Medical apps and wearables gather sensitive and private information, often without the user's knowledge. The private information that a user enters into medical apps or that is collected through a wearable's sensors is also collected, shared, or sold, often without the user's knowledge or consent.[15] A Federal Trade Commission (FTC) study released in May 2014, revealed that just 12 mobile health applications and devices transmitted information to 76 different third parties, and some of the data could be linked

7. Brianna Elliott, *The 10 Best Weight Loss Apps That Help You Shed Pounds*, HEALTHLINE (June 17, 2020), https://www.healthline.com/nutrition/10-best-weight-loss-apps.

8. Lizzy Francis, *10 Stress Management Apps to Help During Hard Times*, YAHOO!LIFE (Mar. 24, 2020), https://www.yahoo.com/lifestyle/10-stress-management-apps-help-191014172.html.

9. Tim Jewell, *The Best Quit Smoking Apps of 2020*, HEALTHLINE (Apr. 25, 2020), https://www.healthline.com/health/quit-smoking/top-iphone-android-apps.

10. Technical Brief 31, *Mobile Applications for Self-Management of Diabetes*, SCI. RES. CTR., (May 8, 2018), https://effectivehealthcare.ahrq.gov/products/diabetes-mobile-devices/technical-brief.

11. Eliza Strickland, *An Official WHO Coronavirus App Will Be a "Waze for COVID-19"*, IEEE SPECTRUM (Mar. 20, 2020), https://spectrum.ieee.org/the-human-os/biomedical/devices/who-official-coronavirus-app-waze-covid19.

12. Philip Brunkard, *Data Privacy And Wearables In Health*, DISRUPTION HUB (Apr. 25, 2018), https://disruptionhub.com/wearables-health-data-bt-philip-brunkard-1653/.

13. *The Precision Medicine Initiative*, WHITE HOUSE, https://obamawhitehouse.archives.gov/precision-medicine (last visited Sept. 21, 2021).

14. *Id.*

15. Jay Hancock, *Workplace wellness programs put employee privacy at risk*, CNN HEALTH (Oct. 2, 2015), https://www.cnn.com/2015/09/28/health/workplace-wellness-privacy-risk-exclusive/index.html.

back to specific users.[16] In addition, 18 third parties received device-specific identifiers, and 22 received other key health information.[17] According to Michelle De Mooy, Deputy Director of the Consumer Privacy Project at the Center for Democracy & Technology, a Washington, D.C. based nonprofit that advocates for civil liberties and human rights on the internet, "health data is more vulnerable in general as a data set than financial data because you can't replace it like you can a credit card."[18]

The larger context reveals the harvesting and monetization of a great deal of our personal information. As FTC Commissioner, Julie Brill noted, "information about some of the most sensitive aspects of our lives is available for analysts to examine without our knowledge or consent."[19] With today's ever-expanding use of technology and the ease with which highly intimate and sensitive information may be acquired and compiled, personal information sometimes may not feel private at all.[20] The FTC has recognized that data brokers consolidate aggregate personally identifiable information (PII) for the purpose of utilizing predictive analytics to discriminate among consumers regarding their race, economic status, and propensity to default or engage in crime.[21] One data broker's database has information on 1.4 billion consumer transactions and over seven hundred billion aggregated data elements; another covers one trillion dollars in consumer transactions; and another adds three billion new records each month.[22] Within these large data brokers, individual profiles have been created on nearly every U.S.

16. Kellog, *supra* note 8.

17. *Id.*

18. Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. B. 76 (2016).

19. Julie Brill, Comm'r, Fed. Trade Comm'n, Keynote Address at the 23rd Computers Freedom and Privacy Conference: Reclaim Your Name (June 26, 2013), https://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf.

20. Lauren Newman, *Keep Your Friends Close and Your Medical Records Closer: Defining the Extent to Which a Constitutional Right to Informational Privacy Protects Medical Records*, 32 J. OF L. AND HEALTH 2; *see also* Lori Andrews, *Use a Health or Medical App? Your Data is Rarely Private*, CHICAGO TRIB. (Aug. 3, 2016), https://www.chicagotribune.com/opinion/commentary/ct-medical-apps-health-privacy-hipaa-perspec-0804-md-20160803-story.html.

21. *See generally Data Brokers: A Call for Transparency and Accountability*, FTC Rep. 8, 46 (2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

22. *Id.* at 46-47.

consumer for the purpose of discriminating between them.[23] The information processing by these data brokers is not sufficiently regulated.[24]

This article will examine the various agencies and statutes that regulate—or fall short of regulating—medical privacy in wearables, and it will also consider the unique privacy concerns of wearables and mHealth apps. Next, this paper will survey the legislative and regulatory landscape to consider the protections afforded to users or lack thereof. Unlike other nations, the privacy legal regime in the United States is highly sectoral, focusing on privacy in particular industries rather than an overall privacy framework. Thus, this paper will consider several pertinent federal laws: the Health Insurance Portability Accountability Act, the Children's Online Privacy Protection Act, and the Stored Communications Act. Next, the paper will consider the authority of the FTC and Food and Drug Administration to regulate in this space and what actions they have taken so far. Additionally, contracts law is a common thread between congressional acts and administrative agencies, so this paper will consider contractual issues that users are bound to, and how a user's "consent" (actual or fictive) allows companies to continue with business practices that imperil users. This paper will further consider security and data breach issues with medical information, specifically the balance between privacy concerns with the potential benefits to the medical community, via precision medicine. Lastly, the paper addresses the benefits and costs of wearables used for contact tracing and symptom diagnosis in light of COVID-19.

The widespread adoption and use of software technologies is opening new and innovative ways that may improve health and health care delivery, but potentially at the cost of substantial invasions of privacy. Some argue that regulation of wearables would stifle innovation and is premature, while others argue new regulation is required now to protect consumers. This paper analyzes how the federal legal framework allows for innovation, regulation, or neither.

23. *Id.* at 46.

24. *See* Mark Andrus, *The New Oil: The Right to Control One's Identity in Light of the Commoditization of the Individual*, AM. BAR ASS'N (Sept. 28, 2017), https://www.americanbar.org/groups/business_law/publications/blt/2017/09/06_andrus/.

Part I: Introduction to Wearables

A. Wearable Technology and Its Function

The wearables market can be broken down into four areas: hearables, smartwatches, wristbands, and "other".[25] Hearables, as defined by the International Data Corporation, are the wearables that hang on or plug into the ear.[26] The device must operate wirelessly and provide stereo sound, while also including at least one of the following features: track health/fitness, modify audio (not just noise reduction), provide language translation on the device, or enable smart assistants.[27] Hearables are expected to grow with a five-year compound annual growth rate (CAGR) of 10.3%, reaching 301.5 million units by 2024.[28] IDC believes hearables are on the cusp of offering health and fitness tracking that would be on par with, or perhaps even better than what, is currently offered on the wrist, since the stationary position of hearables makes them a prime candidate to gather consistent health and fitness data from up and coming sensors.[29]

As for smartwatches and wristbands, these devices include Apple Watches or Fitbits. Lastly, the "other" category is everything else, including smart garments. Because sensors have become inexpensive, manufacturers are including them in increasingly more products, such as smart socks, sports bras, smart bikinis, smart suits (by Samsung), smart glasses, yoga pants, and so on.[30] With the growing variety of wearables, a person's body has become valuable real estate for corporations and app developers to gather their personal information.

B. Scope, Nature, and Context of Data Collected by Wearables

The scope and nature of data collection by apps, wearables, and third parties is substantially broad and significant. Medical apps collect information about the user's thoughts, actions, moods, sex life, responses to interventions,[31] age, name, email address, gender, height, weight, hydration,

25. Michael Shirer, *Worldwide Wearables Market Braces for Short-Term Impact Before Recovery in 2020, According to IDC*, INT'L DATA CORP. (Mar. 16, 2020), https://www.idc.com/getdoc.jsp?containerId=prUS46138520.

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.*

30. *See* Michael Sawh, *The best smart clothing: From biometric shirts to contactless payment jackets*, WAREABLE (Apr. 16, 2018), https://www.wareable.com/smart-clothing/best-smart-clothing.

31. *See, e.g.*, AppAdvice, *DBSA Wellness Tracker: Depression and Bipolar Support Alliance*, APPADVICE, https://appadvice.com/app/dbsa-wellness-tracker/638583516 (last visited Mar. 22, 2020).

diet,[32] exercise habits,[33] online and in-store purchases, whether the user has cable television, who the user phones most frequently, and geolocation.[34] Additionally, data collection is done both actively and passively.[35] Through passive data collection, apps can detect symptoms of COVID-19,[36] the common flu,[37] drug overdoses,[38] Alzheimer's disease,[39] and Huntington's disease.[40] By analyzing such symptoms, the technology might identify a health problem before the user is aware of it. Through measurements of gait, voice, speed, and geolocation, tracking apps and wearables can detect minor changes in the way a user walks, speaks or moves.[41] This might also result in a diagnosis.

This data collection of wearables and mHealth apps has the potential of providing timely notice to enact preventative care, mitigation strategies, and medical planning for users. Additionally, the amount and type of data collected might be helpful to doctors in understanding and detecting varying medical conditions, which could lead to the development of medicines,

32. *See, e.g., 9 Nutrition and Diet Apps for 2020*, KAISER PERMANENTE, https://wa-health.kaiserpermanente.org/best-diet-apps/.

33. *See, e.g.,* Cat Ellis, *The 10 Best Home Workout Apps*, TECHRADAR (Mar. 11, 2020), https://www.techradar.com/best/home-workout-apps.

34. *See, e.g.,* Ashley Hall, *5 Ways to Track Your Personal Health on Your Phone*, VERYWELLHEALTH (Mar. 5, 2020), https://www.verywellhealth.com/track-health-information-phone-1739148.

35. *See* Alexander Seifert, *Mobile Data Collection: Smart, but Not (Yet) Smart Enough*, NAT. CTR FOR BIOTECHNOLOGY (Dec. 18, 2018), at 1; *see also* Liat Clark, *This App Passively Tracks Your Mental Health*, WIRED (Sept. 22, 2014), https://www.wired.co.uk/article/diagnosing-depression-with-an-app. The app strips raw data from the phone's microphone, accelerometer, light sensor and location sensors and runs it through a machine learning algorithm to find patterns in sleep, conversation and activity data.

36. *See* Eric Wicklund, *Scripps Turns to mHealth Wearables to Help Plot Coronavirus Growth*, MHEALTH INTELLIGENCE (Mar. 25, 2020), https://mhealthintelligence.com/news/scripps-turns-to-mhealth-wearables-to-help-plot-coronavirus-growth.

37. *Id.*

38. *See* Angela Chen, *New smartphone app can detect overdoses and call for help*, THE VERGE (Jan. 10, 2019), https://www.theverge.com/2019/1/10/18176994/opioid-overdose-app-sonar-detection-smartphone-technology-science-second-chances.

39. *See* Gina Jordan, *How A Mobile App May Someday Help Diagnose Alzheimer's Disease*, WGCU PUBLIC MEDIA (Oct. 17, 2013), https://news.wgcu.org/post/how-mobile-app-may-someday-help-diagnose-alzheimers-disease.

40. *See id.*; Forest Ray, *Wearable Devices May Aid Diagnosis, But Need Improvement*, HUNTINGTON'S DISEASE NEWS (Mar. 2, 2021), https://huntingtonsdiseasenews.com/2021/03/02/wearable-devices-may-aid-huntingtons-diagnosis-but-evaluation-studies-need-improvement-review-finds/.

41. *See Id.; see also* Jung Hung Chien, *The use of smartphone in measuring stance and gait patterns in patients with orthostatic tremor*, PLOS ONE, July 18, 2019, at 2; s*ee also* Robert J. Ellis, *A Validated Smartphone-Based Assessment of Gait and Gait Variability in Parkinson's Disease*, PLOS ONE, Oct. 30, 2015, at 1-2.

preventive care, and pharmaceuticals.[42] However, despite mHealth apps' potential benefits, the use of these tools has been limited, as most people stop using them after a short period of time.[43] Wearables, on the other hand, are not as easily discarded because they serve a particular valued function, *e.g.*, telling time or listening to music. Unlike phone apps, the continued use of smartwatches, ear pods, wristbands, and smart clothes may withstand the pitfalls of apps, which means their data collection would continue. However, it is not yet certain whether the potential benefits of wearables will result in better health outcomes for their users.

Nevertheless, potential health benefits of wearables need to be balanced against privacy concerns. Existing data-collection efforts by private parties such as data brokers and aggregators, search engines, and social media giants far exceed anything that Congress has attempted to regulate in consumer-protection statutes such as the Fair Credit Reporting Act (FCRA) or other consumer-protection statutes.[44] Because of the lack of legislation and regulation regarding wearable-generated health data, companies sell this information to data aggregators and brokers with impunity.[45] The sharing of this sensitive, medical information can lead to higher insurance rates or job discrimination. [46] Dr. Jesse M. Ehrenfeld, chair of the American Medical Association board, stated, "patients simply may not realize that their genetic, reproductive health, substance abuse disorder, [and] mental health information can be used in ways that could ultimately limit their access to health insurance, life insurance, or even be disclosed to their employer.… Patient privacy can't be retrieved once it's lost."[47]

Companies have long processed consumer data in order to deliver targeted ads—and thereby intruded on consumer privacy. To illustrate how this personal information eerily impacted one unsuspecting father, one needs only look so far as a Target located in Minneapolis. After receiving a Target ad, a father angrily stormed into a Target. He demanded to know from the manager why his daughter, who was still in high school, was receiving ads for maternity clothing and nursery furniture – it turned out that his daughter

42. *See* Ellis, *supra* at 2.

43. *See* Gunther Eysenbach, *The Continued Use of Mobile Health Apps: Insights From a Longitudinal Study*, JMIR MHEALTH UHEALTH, Aug. 2019, at 1.

44. Andrus, *supra* note 23.

45. Natasha Singer, *When Apps Get Your Medical Data, Your Privacy May Go With It*, N.Y. TIMES (Sept. 3, 2019), https://www.nytimes.com/2019/09/03/technology/smartphone-medical-records.html.

46. *Id.*

47. *Id.*

was in fact pregnant.[48] Target created an algorithm that used items purchased to predict when a consumer was pregnant, including an accurate prediction of their due date.[49] In this instance, Target's algorithm analyzed women's purchases of a combination of unscented lotion, cotton balls, and mineral supplements.[50] The combination of behaviors may go overlooked to a user, but could be gold for a company because it provides them with data to deliver a precisely timed advertisement that can change someone's shopping patterns at a pivotal moment, potentially resulting in changed shopping behavior for years.[51]

The privacy risks are heightened with health data. A patient who uses a health app or wearable might be unaware of their symptoms, or the diagnosis based on those symptoms. The device, however, can document the symptoms, or even make a diagnosis, and then transmit all that information to a third party. Unsurprisingly, the value of medical information on the black market is fifty times that of credit card information.[52]

The context of how wearables and apps collect sensitive health information is also important. Traditionally, disclosure of medical information from a client to a doctor occurred in the privacy of her office. The client had control over what symptoms or information they chose to disclose. As for doctors, there are substantial regulations that they must adhere to. First, doctors swear to an ethical standard when they make the Hippocratic oath.[53] There is a doctor-patient confidentiality relationship that a doctor is bound to uphold through both common law and state statutes.[54] Additionally, doctors are bound by common law doctrines of privacy,

48. Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#45d8b7896668.

49. *Id.*

50. *Id.*

51. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

52. *See* Consumer Reports, *Hackers Can Profit Greatly by Stealing Your Health Data. Are You Protected?*, WASH. POST (Nov. 9, 2015), https://www.washingtonpost.com/national/health-science/hackers-can-profitgreatly-

by-stealing-your-health-data-are-you-protected/2015/11/09/e1f126f6-5181-11e5-933e-7d06c647a395_story.html?utm_term=.ccf13bc3b1c3.

53. *The Hippocratic Oath*, INDIAN J. OF MED. ETHICS (Aug. 1, 1993), https://ijme.in/articles/the-hippocratic-oath/?galley=html.

54. *Doctor Patient Confidentiality*, USLEGAL, https://healthcare.uslegal.com/doctor-patient-confidentiality/.

fiduciary duty,[55] contract, negligence,[56] and warranty.[57] Thus, if a doctor violates patient privacy, they can be fined, penalized, or held civilly liable. These safeguards engender trust, which is essential for prevention, diagnosis, and treatment. These safeguards are not present with wearables, which are made by companies not covered by doctor-patient privacy rules.

Part II: Sectoral Privacy Laws in the United States

A. Health Insurance Portability and Accountability Act

When dealing with medical information, the Health Insurance Portability and Accountability Act (HIPAA) is the first piece of federal legislation to consider. The Act's focus is on the health industry. In 1996, Congress enacted HIPAA to safeguard health information while also encouraging doctors to move to electronic files.[58] Further, HIPAA's purpose is to improve the Federal Medicare and Medicaid programs as well as the efficiency and effectiveness of the health information system through the establishment of standards and requirements.[59]

These standards include notice, protecting personal health information (PHI), and proper release of PHI.[60] PHI includes any individually identifiable information maintained or transmitted by a "covered entity" or a "business associate" that relates to an individual's physical or mental health or the provisions of or payment for healthcare.[61] HIPAA defines a "covered entity" as healthcare providers, health plans, or healthcare clearing houses who *electronically* transmit any health information in connection with a transaction covered by HIPAA.[62] A covered entity must comply with HIPAA Rule requirements. A "business associate" is defined as a person or entity that creates, receives, maintains, or transmits PHI on behalf of a covered

55. Jeff Brown, *Doctors owe their patients some fiduciary responsibility*, KEVINMD.COM (Jan. 7, 2010), https://www.kevinmd.com/blog/2010/01/doctors-owe-patients-fiduciary-responsibility.html.

56. Frank C. Spencer, *The Medical Malpractice Crisis*, ETHICS J. OF THE AM. MED. ASS'N Vol. 7, No. 4 (April 2004), available at https://journalofethics.ama-assn.org/article/malpractice-crisis/2005-04.

57. *Duty of physician—Basis of duty—Warranty*, 3 Modern Tort Law: Liability and Litigation § 24:17 (2d ed.).

58. *See generally* Shaun G. Jamison, *Creating A National Data Privacy Law for the United States*, 10 CYBARIS AN INTELL. PROP. L. REV. 1, 10 (2019).

59. *Yath v. Fairview Clinics, N.P.*, 767 N.W.2d 34, 49 (Minn. Ct. App. 2009).

60. Jamison, *supra* note 55.

61. 45 C.F.R. § 160.103 (2014). *See generally* Cristina M. Mares, *To Cover or Not to Cover? The Relationship Between the Apple Watch and the Health Insurance Portability and Accountability Act*, 18 DEPAUL J. HEALTH CARE L. 159, 162 (2016).

62. *See* 45 C.F.R. § 160.103 (defining "covered entity").

entity.[63] A covered entity that engages a business associate must have a written contract that specifically establishes what the business associate has been engaged to do and requires the business associate's compliance with HIPAA.[64]

Generally, a company that develops, sells, or manufactures an mHealth app or wearable does not qualify as a HIPAA-covered entity. Such a company typically is not a medical provider, health plan, or health clearinghouse. Nor are they considered business associates because they do not communicate information to a covered entity.[65]

Nonetheless, some aspects of mHealth apps and wearables may require HIPAA compliance. For example, every iPhone comes with particular apps pre-installed, including Health and MyChart.[66] The Health app is a fitness tracker that counts steps and measures walking and running distances. When paired with an Apple Watch, this app automatically tracks activity data.[67] MyChart provides fast, secure access to a users' medical records, the ability to send private messages to physicians and other health providers, to see upcoming and past appointments, to view and pay medical bills, to get lab results, and to pull health-related data from personal devices right into MyChart.[68] The federal government is working to complete rules to require health providers to send medical information to third-party apps, like MyChart, after a patient has authorized the data exchange.[69] HIPAA would potentially apply to MyChart if it communicates PHI to a health service

63. *See* 45 C.F.R. § 160.103 (declaring the meaning of "business associate").

64. *See* Mares, *supra* note 59 (describing the scope of data collection for a "business associate").

65. Kellog, *supra* note 6 at 2; *see also* Mark D. Rasch, *Privacy and Security in the Internet-Connected World of Precision Medicine*, ABA SCITECH LAW., Fall 2018, at 18, 21; *but see* Fred Donovan, *How Does HIPAA Apply to Wearable Health Technology*, HEALTHITSECURITY (July 24, 2018), https://healthitsecurity.com/news/how-does-hipaa-apply-to-wearable-health-technology.

66. Erik Lorenzsonn, *Apple steps into Epic Systems' arena with medical records iPhone*, CAP. TIMES (Jan. 27, 2018), https://madison.com/ct/business/technology/apple-steps-into-epic-systems-arena-with-medical-records-iphone/article_3875e65b-2cb1-5ceb-9e6d-601fa66af77b.html.

67. User Directions, *Use the Health app on your iPhone or iPod touch*, APPLE (Feb. 1, 2021), https://support.apple.com/en-us/HT203037.

68. Apple, *MyChart*, App Store Preview, https://apps.apple.com/us/app/mychart/id382952264#?platform=appleWatch (last visited Apr. 19, 2020).

69. Singer, *supra* note 42. ("The regulations are part of a government effort to push health providers to use and share electronic health records. Regulators have long hoped that centralizing medical data online would let doctors get a fuller, more accurate picture of patient health and help people make more informed medical choices, with the promise of better health outcomes. Dr. Rucker, of the federal health department's national coordinator for health information technology, said it was self-serving for physicians and hospitals, which may benefit financially from keeping patients and their data captive, to play up privacy concerns.").

provider. On the other hand, if the PHI remains on the phone or is communicated to a party other than a service provider, the data is not protected by HIPAA.

For another example of how HIPAA might apply to mHealth, consider the 2017 agreement between the National Football League Players Association (NFLPA) and Whoop, a wearable-technology company.[70] An officially licensed NFLPA wearable is provided to each NFL player with the goal of studying the effects of travel, sleep, scheduling, and injuries on players' recovery.[71] The goal is to provide players, trainers, and coaches with a detailed analysis of a player's body preparedness, while ensuring each player owns and controls his data.[72] With the data collected, trainers and coaches can customize a player's training.

With such a large amount of sensitive data of high-profile individuals, does HIPAA apply? Well, each club is required to have board-certified medical personnel, which are required to comply with local, state, and federal law.[73] Thus, each football team likely qualifies as a covered entity. The information collected from the wearable did not stay on the device, but rather was transmitted to the trainers, doctors, and coaches, which is essentially the team, a covered entity. Therefore, HIPAA likely applies. If, however, the information remained on the device, it would not be communicated to a covered entity and would not be protected by HIPAA. As to Whoop, it would be considered a business associate of each team, so the information it collects would also be covered by HIPAA. Further, even if the information were not protected by HIPAA, Whoop entered into a contractual agreement with the players wherein each player owns their information.

However, the average consumer of wearables is not an NFL player with a team of doctors that triggers HIPAA, or is not engaged contractual relationship that provides ownership of data. Regarding the NFLPA, Whoop was likely incentivized to provide these significant protections to gain publicity in order to increase sales and profit. The protections afforded to NFLPA vary drastically from the terms for ordinary users.[74] Thus, although

70. Terence M. Durkin, *Health Data Privacy and Security in the Age of Wearable Tech: Privacy and Security Concerns for the NFLPA and Whoop*, 19 J. HIGH TECH. L. 279, 281 (2019).

71. *Id.*

72. *Id.* at 282.

73. *Id.* at 297.

74. *Terms of Use*, WHOOP, https://healthitsecurity.com/news/how-does-hipaa-apply-to-wearable-health-technology (last visited May 5, 2020) (Whoops' term of use state: "By submitting the User Content to us, you hereby grant us a perpetual, worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to edit, modify, truncate, aggregate, use, reproduce, distribute, prepare derivative works of, modify, display, perform, publish and otherwise commercially exploit all or any portion of the User Content in connection with our provision of the

Whoop is capable of providing significant protections to all users, as they did with the NFLPA, they generally do not.

To implement HIPAA, the Department of Health and Human Services (HHS) issued regulations regarding the protection of PHI, known as the "Privacy Rule."[75] In 2009, the Health Information Technology for Economic and Clinical Health Act (HITECH) expanded HIPAA protections. For example, it requires covered entities to notify clients regarding breaches of unsecured information and make certain HIPAA privacy requirements applicable to business associates.[76] Like HIPAA itself, the Privacy Rule extends only to covered entities and business associates.[77]

Additionally, HHS issued the "Security Rule" to protect the confidentiality, integrity, and availability of PHI when it is stored, maintained, or transmitted.[78] The Security Rule requires that covered entities protect against any reasonably anticipated threats or hazards to the security or integrity of the PHI. It also provides that certain uses or disclosures of PHI are not permitted or required.[79] Covered entities are liable for improperly disclosed PHI pursuant to HIPAA, whether disclosure was intentional or merely negligent.[80] The Privacy Rule and Security Rule work hand-in-hand in the event of a security breach.

The consequences of a security breach or hack of a wearable can be devastating to a user since medical, geolocation, and other information may be stored on the device. However, because most wearables are not currently covered by HIPAA, the Security Rule and Privacy Rule do not apply. Wearables have significant security vulnerabilities. For example, wearables connect to a phone via Bluetooth, and Bluetooth connectivity provides an avenue for a hacker to infiltrate. Security researcher Axelle Apvrille claims she was able to hack a Fitbit bracelet in 10 seconds from 15 feet away.[81] Yet,

Services and our (and our successors') business, including without limitation for promoting and redistributing part or all of the Services (and derivative works thereof) in any media formats and through any media channels and sharing the User Content with social media platforms (i.e., posting User Content to Twitter or Facebook if enabled in your Account's sharing settings) with our business partners and licensees for informational and analytical purposes. If your use of the Services is on behalf of or managed by a coach, team, organizing body or other entity you are affiliated with ("Managing Entity"), your User Content may also be shared with that team or other organization as more fully described in our Privacy Policy." With these terms, Whoop essentially acquires complete ownership of the users data.).

75. HIPAA Privacy Rule, Practical Law Practice Note 4-501-7220 (1996).

76. *Id.*

77. *Id.*

78. HIPAA Security Rule, Practical Law Practice Note 5-502-1269 (1996).

79. *Id.*

80. *Id.*

81. Alexandra Burlacu, *Experts Warn It Just Takes 10 Seconds to Hack Fitbit Fitness Trackers: Here's Fitbit's Response*, TECH TIMES (Oct. 24, 2015),

HIPAA does not apply to a wearable breach unless there is some connection or transmission to a covered entity.

Ultimately, with minor exceptions, HIPAA does not cover wearables. Wearables are capable of gathering a vast amount of sensitive health information that can jeopardize the future of a consumer once the information is sold or shared with a third-party that is not a covered entity or business associate.

B. Children's Online Privacy Protection Act

In 1998, Congress enacted the Children's Online Privacy Protection Act (COPPA). This act stems from the public policy of protecting children because they are a vulnerable population.[82] COPPA requires parental consent before certain types of information is collected about their children, while completely barring collection of other types of information.[83]

Under COPPA, any website either directed at children (under 13 years of age) or knowingly collecting personal information from such children must: (1) "provide notice on the website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information"; and (2) "obtain verifiable parental consent for the collection, use, or disclosure of personal information from children."[84] Additionally, at a parent's request, a website must describe what type of personal information was collected from that parent's child, give that parent the opportunity to bar the website's further use of the information collected, and give the parent access to the information.[85] Companies also may not require a child to submit more information than is reasonably necessary.[86] In 2019, the FTC and YouTube reached a $170 million settlement for alleged COPPA violations.[87] The FTC

http://www.techtimes.com/articles/98427/20151024/experts-warn-it-just-takes-10-seconds-to-hackfitbit-fitness-trackers-heres-fitbits-response.htm.

82. *See Complying with COPPA: Frequently Asked Questions*, FTC (Mar. 20, 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Questions.

83. HIPAA Privacy Rule, *supra* note 74; *see also* Jamison, *supra* note 57, at 8.

84. 15 U.S.C. § 6502(b)(1)(A)(i)–(ii)(1998).

85. *Id*.

86. 15 U.S.C. § 6502(b)(1)(C); s*ee also Yelp, TinyCo Settle FTC Charges Their Apps Improperly Collected Children's Personal Information,* FTC (Sept. 17, 2014) https://www.ftc.gov/news-events/press-releases/2014/09/yelp-tinyco-settle-ftc-charges-their-apps-improperly-collected (Tinyco, a games developer, failed to comply with COPAA requirements by requiring children to provide an email address for extra game points. In another case, Yelp was aware that children were using its app and website, resulting in Yelp adopting an age gate for access. Yelp, however, implemented the age gate incorrectly).

87. *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law*, FTC (Sept. 4, 2019), https://www.ftc.gov/news-events/press-

and New York Attorney General had alleged YouTube used cookies on viewers of child-directed channels, without first notifying parents and obtaining consent.[88] The COPPA Rule addresses persistent identifiers like cookies that track a user's internet browsing habits for targeted advertising.[89]

With the popularity of wearables and the trajectory of market expansion,[90] the wearables market may increasingly cater to a younger audience. Children's wearables currently include GPS trackers, baby monitors, fitness trackers,[91] smart rings, watches, and bracelets.[92] In developing this technology, companies should give special attention to the privacy interests of children. Developers have an opportunity to consider privacy from the inception of the device and incorporate privacy solutions at the hardware level. Yet, many companies have foregone this opportunity.[93]

Although COPPA requires parental consent, once this consent is obtained, the company can then use, store, or sell the information collected. Consent is often obtained through the all too familiar "clickwrap" agreement, which comes in the form of a contract or terms of use followed by with words "I accept" and a small checkbox. Courts generally find clickwrap agreements to be enforceable because they necessitate an active role by the user.[94] However, the privacy policies that companies provide to parents are often lengthy, confusing, and tend to obfuscate and bury how data storage and collection actually operate.[95] This makes it exceptionally difficult for consumers to understand how features on a device, and the information collected therein, operate and relate to the privacy policy.[96] Studies show that 74% of adults skip privacy policies and simply agree to the terms without

releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations. (The settlement also requires YouTube develop, implement, and maintain a system that permits channel owners to identify their child-directed content so that YouTube can ensure it is complying with COPPA.)

88. *Id.*

89. *Id.*

90. Shirer, *supra* note 24.

91. Fitbit, *Ace 2*, FIBTBIT STORE, https://www.fitbit.com/us/products/trackers/ace2 (last visited Apr. 20, 2020).

92. Safety Team, *Safety.com's Top 10 Wearables for Kids*, SAFETY.COM (Mar. 9, 2020), https://www.safety.com/best-wearables/ (last visited Apr. 29, 2020).

93. Husain Sumra, *Kids smartwatch makers are in trouble for collecting data without permission*, WAREABLE (Apr. 30, 2018), https://www.wareable.com/smartwatches/gator-tinitell-ftc-warning-kids-data-2018.

94. Berkson v. Gogo LLC, 97 F. Supp. 3d 359, 397 (E.D.N.Y. 2015).

95. James Gilmore, *Securing the Kids: Geofencing and Child Wearables*, 26 CONVERGENCE INT. J. OF RSCH. INTO NEW MEDIA TECH. 1333, 1340-41 (2019).

96. *Id.*

reading them.[97] For example, Jiobit, a children's GPS device, stresses that geolocation data is never shared for marketing purposes, but then states in their privacy policy that personal information could be shared with "'third parties who may contact you about our products and services that may be of interest to you, as well as incorporating interest-based ads . . . presented to you based on your browsing behavior in order to provide you with ads more tailored to your interest."[98]

Thus, with parental consent, children's data can be used for marketing purposes, and even sold. Nevertheless, so-called "consent" to such processing of children's mHealth data will often not be genuine consent. The terms of use agreements incorporate complicated privacy policies that parents often click through without actually understanding. Because terms of use agreements bury important terms within clickwrap agreements, true informed consent is often not obtained. Courts are upholding these agreements because the user plays an active role in providing consent.[99] Consequently, a datafication of children is occurring despite COPPA. Additionally, because COPPA requires parental consent, children lack agency in the decision to assent to the terms of use of the wearable. The assumption is that parents are better positioned to make this decision, but this assumption is questionable with complex privacy policies and terms of use. The gap between the purpose of COPPA and reality can potentially be addressed by designing privacy features from inception or, at the least, draft plain English privacy policies that require more than checking a box.

C. Stored Communications Act

Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA).[100] ECPA includes the Stored Communications Act (SCA).[101] The SCA is an important statutory protection of the privacy of digital communications and data.[102] It regulates two kinds of entities: "remote computing services" (RCS), which provide computer storage or processing services by means of an electronic communication system; and "electronic

97. Oeldorf-Hirsch et al., *Overwhelming, Important, Irrelevant: Terms of Service and Privacy Policy Reading Among Older Adults*, 2019 SMSociety '19: Proc. of the 10th Int'l Conf. on Soc. Media and Soc'y. 166, 169.

98. Gilmore, *supra* note 94, at 1341.

99. *Compare with* Nguyen v. Barnes & Noble Inc., 763 F.3d 1171, 1178 (9th Cir. 2014). Courts have generally not enforced browsewrap agreements because users do not play an active role in providing consent.

100. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 2510, 100 Stat. 1848 (amended 1986).

101. *Id.*

102. *See generally* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

communications services" (ECS), which provide the ability to send or receive wire or electronic communications.[103] The SCA limits when such entities can disclose two kinds of digital information: "contents," which are the substance or meaning of a communication; and "records," which are metadata, such as who wrote to whom and when.[104] The SCA limits disclosures of content to non-government entities, but does not limit disclosures of records to non-government entities.[105] The SCA requires a warrant for disclosure of content to government and requires a court order based on "reasonable grounds" of "relevance" to disclose records to the government.[106]

The SCA applies to consumer wearables if the health app at issue provides either an RCS or ECS.[107] Particularly of importance, the SCA restrictions only apply if the service is provided "to the public."[108] Services are provided "to the public" if they are generally available and not exclusive.[109] For example, social media is public because anyone can download it, whereas internal networks at a corporation are non-public because employment is required for access.

If the SCA applies to a wearable, the next question is whether the user's information is "content" or "records." If a person uses a wearable to send a text message, social media post, or email, that would probably be considered "content." On the other hand, if a wearable's sensors generated information about a user by monitoring their workout or geolocation, that would probably be considered "records." Most data collected from wearables would be considered records and not content.[110] Under the SCA, records can freely be transmitted to third parties, including data brokers, without the users' consent.[111] Congress could protect user privacy in the context of wearables by expanding the definition of "content" or increasing the protection of "records." However, even then, companies and developers could still disclose wearable-generated consumer data with a user's consent.[112] As with COPPA, this would require the ill-equipped user to interpret complicated

103. 18 U.S.C.A. § 2711(1)-(2); 18 U.S.C.A. § 2510(15).

104. 18 U.S.C.A. § 2702(a); 18 U.S.C.A. 2510(8).

105. 18 U.S.C.A. § 2702(a)(3).

106. 18 U.S.C.A, §§ 2702(a), (b)(2), and (c)(1); 18 U.S.C.A. §§ 2703(a), (b), (c)(1)(B), (d).

107. Durkin, *supra* note 67 at 3.

108. 18 U.S.C.A. § 2702(a). *See also* Kerr, *supra* note 155 at 1231.

109. *Id.* at 1226.

110. Durkin, *supra* note 67 at 3; *see also* Nayanika Challa, *Wary About Wearables: Potential for the Exploitation of Wearable Health Technology Through Employee Discrimination and Sales to Third Parties*, 10 No. 3 INTERSECT: THE STAN. J. OF SCI., TECH., AND SOC'Y (2017).

111. Kerr, *supra* note 102 at 1220-22.

112. 18 U.S.C.A. § 2702(b)(3) & (c)(2); *see also* Kerr, *infra* note 162 at 1221.

policies with little choice or leverage. Because of the complexity and deliberate obfuscation of user agreements, such legal protection alone might not be effective.

Part III: Administrative Regulation

Two administrative agencies, the Federal Trade Commission and the Food and Drug Administration, have regulatory powers that relate to mHealth. Unfortunately, neither has provided significant privacy protection for users of wearable devices.

A. Federal Trade Commission Act

The Federal Trade Commission (FTC) has the authority, per Section Five of the FTC Act, to enforce cease-and-desist orders against any entity for "unfair or deceptive acts or practices" that pertain to data management.[113] Since the passage of the Fair Credit Reporting Act (FCRA), the FTC has been the chief federal agency on privacy policy and enforcement.[114] In order to act, the FTC analyzes whether the business act "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[115] Deceptive acts or practices occur "if there is a representation, omission, or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer's detriment."[116]

The FTC's approach to privacy protection can be illustrated by three of its enforcement actions under Section Five, and by its development of "fair information practice principles." As explained below, these FTC measures have not done enough to protect privacy, because they rely on users' so-called "consent" to lengthy privacy policies that users cannot reasonably be expected to understand. Thus, the FTC's traditional approach to privacy protection might not be sufficient to secure the vast amounts of sensitive medical information already being generated by mHealth apps and wearables.

113. Federal Trade Commission Act, 15 U.S.C. § 45(b) (2006). Outside of protecting consumers, the FTC leads studies, facilitates workshops, and issues reports on technology related topics. Annually, the FTC hosts Privacycon, where recent research on privacy and security issues are presented by leading scholars, researchers, industry representatives, consumer advocates, and the government.

114. *Protecting Consumer Privacy and Security*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy-security (last visited Apr. 20, 2020).

115. 15 U.S.C. § 45(n).

116. *Zlotnick v. Premier Sales Grp., Inc.*, 480 F.3d 1281, 1284 (11th Cir. 2007).

B. F.T.C v. Wyndham

In *F.T.C. v. Wyndham,* the case challenged 15 U.S.C. § 45 as being so vague that it could not be enforced.[117] The court held that this provision of the FTC Act sufficiently informs parties that the relevant inquiry is a cost-benefit analysis, which considers a number of relevant factors. These factors include the probability and expected size of reasonably unavoidable harms to consumers given a certain level of cybersecurity and the costs to consumers that arise from investment in stronger cybersecurity.[118] Additionally, the FTC's authority to enforce privacy actions was unsuccessfully challenged. This decision exemplifies that the FTC's authority is broad and applies to both cybersecurity and misleading privacy policies.[119]

C. Goldenshores Technologies

In 2014, the FTC used its Section Five authority against Goldenshores Technologies' Brightest Flashlight Free app for deceiving customers. The privacy policy allegedly did not reflect the app's use of personal data and presented consumers with a false choice on whether to share their information.[120] The FTC's complaint asserted that the app was downloaded tens of millions of times. The complaint also claimed that Goldenshores' privacy policy did not adequately disclose that "the Brightest Flashlight App transmits or allows the transmission of device data, including precise geolocation along with persistent device identifiers, to third parties, including advertising networks."[121] Under the settlement, Goldenshores was prohibited from misrepresenting how consumers' information is collected, shared, and used; required to provide a just-in-time disclosure that "fully informs consumers, when, how, and why their geolocation information is being collected, used, and shared"; required to obtain consumers' affirmative consent; and required to delete any personal information collected through the Brightest Flashlight app.[122]

The Goldenshores case illustrates that the FTC has authority to regulate deceptive and fraudulent actions. Had Goldenshores fully disclosed their data collection and business practices in their terms of use policy, they could

117. *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 250 (3d Cir. 2015).

118. *Id*. at 255.

119. *See Id.*; *see also* Jamison, *supra* note 55.

120. *FTC Approves Final Order Settling Charges against Flashlight App Creator*, FTC (Apr. 9, 2014), https://www.ftc.gov/news-events/press-releases/2014/04/ftc-approves-final-order-settling-charges-against-flashlight-app.

121. Complaint at 3, In re Goldenshores Techs., LLC, Erik M. Geidl, FTC No. 132-3087 (Dec. 5, 2013).

122. F.T.C., *supra* note 118.

have avoided this FTC enforcement action. As such, the FTC is encouraging full disclosure. This again shifts the responsibility to consumers, but consumers are not always in the best position to interpret policies and provide informed consent to such policies.

App permissions are typically confusing and unclear. Each app typically has a list of permissions that are granted to the developer when the user downloads an app to a device. Most app users do not understand permissions and tend to avoid them when downloading and installing apps.[123] Even security experts find that permissions are sometimes incomprehensible.[124]

Yet, permissions have serious consequences because many apps are overprivileged and overreaching in a way that provides apps access to information that do not correspond to the functionality of the app.[125] For example, most apps that obtain permission to track location do not need location data to provide app functionality to the user.[126] Other app permissions authorize app developers to record audio, read contacts on the phone, and take pictures.[127] This information is a goldmine for companies because they can then sell it to advertisers. In one study, experts found that of 940 Android apps, nearly one-third had overreaching permissions.[128]

One distinguishing feature between these apps is whether it is a paid or free app. In a study of 99 apps, researchers found that free apps included more unnecessary permissions than paid apps.[129] This difference is likely attributable to the varying business models of how profits are derived; that is, either from advertising revenue or directly from the user.

D. Trendnet

Trendnet is a California corporation that sells networking devices, such as routers, modems, and internet protocol (IP) cameras, to home users and mid-size businesses.[130] From 2010 to 2012, Trendnet made a total revenue

123. Andrews, *infra* note 178, at 439.

124. *Id.*

125. *Id.* at 440.

126. *Id.* In another example, a diabetes recipe app allowed the app to "find user accounts on the phone; read and modify contacts; read the calendar; track the user's precise (GPS-based) location; make phone calls; read and modify the call log; test access to and modify external storage; obtain the device ID; activate the camera and microphone, and install and delete other applications."

127. *Id.*

128. *Id.*

129. *Id.* at 441.

130. Complaint at 2, In re Trendnet Inc., F.T.C. File No. 122 3090 (Jan. 16, 2014) (No. C-44), https://www.ftc.gov/system/files/documents/cases/140207trendnetcmpt.pdf; *See also*, Jessica Kitain, *Beware of Wearables: Protecting Privacy in A Data-Collecting World*, 9 DREXEL L. REV. ONLINE 1, 23 (2017).

of $192 million, including $19 million from IP cameras.[131] The function of these cameras is to "conduct security monitoring of [a person's] home or business, by accessing live video or audio feeds from their cameras over the internet."[132] Access to the camera requires login credentials, but this requirement can be disabled.[133] Trendnet described its IP cameras as secure.[134] For example, Trendnet affixes a sticker to the cameras packaging of a lock with the capitalized word "SECURITY".[135]

Yet Trendnet failed to provide a secure product, including failing to implement even the most basic security measures.[136] Trendnet stored "user login credentials in clear, readable text over the internet," "failed to implement a security process to monitor security vulnerabilities," and "failed to employ reasonable and appropriate security in the design and testing."[137] Because of their failings, hackers compromised hundreds of IP cameras and posted live feeds for nearly 700 IP cameras.[138] The live feeds displayed "'private areas of users' homes and allowed the unauthorized surveillance of infants sleeping in their cribs, young children playing, and adults engaging in typical daily activities."[139]

The FTC instituted a consent order composed of nine parts. Part I forbids misleading consumers about the security of the device and security, privacy, confidentiality, or integrity of any consumer information.[140] Part II requires Trendnet to maintain a security program to "(1) address security risks that could result in unauthorized access to or use of Covered Device Functionality, and (2) protect the security, confidentiality, and integrity of Covered Information."[141] Part III requires Trendnet to complete assessments (by a third party) every other year to review compliance with the consent order.[142] Part IV requires Trendnet to notify consumers of camera and security flaws, offer free and prompt support, and help consumers uninstall

131. *Id.* at 2.
132. *Id.*
133. *Id.*
134. *Id.* at 3.
135. *Id*.
136. *Id.*
137. *Id.* at 4.
138. *Id.* at 5.
139. *Id.*
140. *Id.* at 5.
141. *Id.*
142. *Id.*

cameras.[143] Parts V through IX require Trendnet to repeatedly report to the FTC.[144] The consent order will remain in effect for twenty years.[145]

Trendnet sets the baseline that companies must abide by to avoid FTC actions for lack of security protections. Ultimately, providing security protections helps both the consumer and the company. If consumers do not feel secure with technology that collects sensitive information, consumers will shift to another platform. Conversely, had the FTC not taken action, it would have invited adverse companies into the marketplace that otherwise could not develop appropriate security requirements, which would likely sell at a lower price and undercut more secure technologies. Additionally, consumers would likely not be in a position to discern between the security features, which would result in potential security breaches of the home. The home is an area courts hold to be where citizens have the most privacy concerns.[146]

* * *

The three cases above illustrate the significant authority the FTC has to address privacy and security concerns in apps and devices. In one more example, *FTC v. Frostwire, LLC*, the settlement barred the company from using default settings to cause inadvertent public sharing of files by consumers and required clear and prominent disclosures of file sharing and how to disable it.[147]

Yet, despite having the authority to launch investigations into medical apps and wearables that are sharing information with data aggregators and brokers, the FTC has "generally chosen to take action only when an app developer [or device manufacturer] fails to disclose in advance that it will be invading a person's privacy."[148] Likewise, the FTC will not seek judgments against companies that fully disclose their practices in their privacy policies, terms of use, or other documents, because it would no longer be "unfair or deceptive."[149]

Under this enforcement strategy, the onus shifts from the company to the consumer, who is then tasked with carefully reading complex privacy policies. However, more than 80% percent of users do not always read their

143. *Id*. at 6.

144. Kitain, *supra* note 97, at 23.

145. *Id.*

146. *Florida v. Jardines*, 569 U.S. 1, 1 (2013).

147. Andrews, *supra* note 181, at 448 (The FTC has also secured consent decrees against Facebook, Snapchat, LabMD, and Wyndham Worldwide for similar violations).

148. *Id.*

149. *Id.*

privacy policies and only 19% are aware of circumstances where their personal data was used in a way they did not expect.[150] Given these facts, the FTC might not adequately protect users of wearables and mHealth apps from having their medical information inappropriately shared, because privacy policies can be deliberately confusing, overreaching, or present no meaningful opportunity for individual choice.[151] As mentioned previously, the FTC has the authority to prosecute "deceptive and fraudulent" business practices; however, the FTC has been selective in its enforcement.[152] The FTC has brought actions against clear acts of deception, such as by Trendnet and Goldenshores, but has left a large segment of the market untouched with apps that grant themselves overreaching permissions.[153]

E. Fair Information Practice Guidelines

In its 1998 report, *Privacy Online: A Report to Congress*, the FTC summarized widely accepted principles, known as "fair information practice principles" (FIPPs), regarding the collection, use, and dissemination of personal information.[154] In May 2000, the FTC added to and refined these principles, which included notice, choice, access, security, and enforcement.[155] For notice, "Web sites would be required to provide consumers clear and conspicuous notice of their information practices."[156] For choice, "Web sites would be required to offer consumers choices as to how their personal identifying information is used beyond the use for which the information was provided (e.g., to consummate a transaction)."[157] For access, "Web sites would be required to offer consumers reasonable access

150. Report, *Global Internet User Survey Summary Report*, INTERNET SOC'Y, 448 (2012), https://wayback.archive-it.org/9367/20170907075239/https://www.internetsociety.org/sites/default/files/GUIS-2012-Infographic.pdf (last visited Apr. 19, 2020).

151. *Id.* at 449.

152. *Supra* note 146 at 449.

153. *See* Andrews, *supra* note 181, at 439. "Permissions authorize app developers to access sensitive information, such as the ability to track the user's location (18% of diabetes apps), record audio (4%), read contacts on the phone (6%), and take pictures (11%).110 The permissions for bipolar apps in our study included finding accounts on the device (25%), reading the user's contacts (8%), seeing their precise location (17%), modifying or editing the contents of the phone's USB storage (62%), recording audio (5%), and taking pictures or videos (13%)."

154. *See Privacy Online: A Report to Congress*, FTC, at 3 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

155. *See Privacy Online: Fair Information Practices in the Electronic Marketplace—A Report to Congress*, FTC (2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000text.pdf.

156. *Id.* at 34.

157. *Id.*

to the information a Web site has collected about them."[158] For security, "Web sites would be required to take reasonable steps to protect the security of the information they collect from consumers."[159] For enforcement, the FTC identified three types of measures: self-regulation by the information collectors or an appointed regulatory body; private remedies that give civil causes of action for individuals whose information has been misused to sue violators; and government enforcement that can include civil and criminal penalties levied by the government.[160]

Although theoretically appealing, FIPPs have often been an unsuccessful approach to privacy issues.[161] Users undergo a blitz of notices and opportunities for generally limited choice.[162] For many users, notices do not serve a helpful purpose because they are either ignored or overly complicated.[163] Many users do not want to be burdened with impenetrable choices when they are downloading an app. Some people avoid making choices as to what data is collected and try to circumvent notices of such a choice.[164] Other people, when confronted with a choice, are ill-equipped to make an informed decision.[165] Ultimately, as Fred H. Cate argues, the illusion of privacy under a FIPPs regime creates the worst of both worlds: "privacy protection is not enhanced, individuals and businesses pay the cost of bureaucratic laws, and we have become so enamored with notice and choice that we have failed to develop better alternatives."[166] On the other hand, as to how credit information is gathered, shared, and used, the Fair Credit Reporting Act (FCRA) assigns greater responsibility to the businesses and less to the consumer.[167] This makes sense because businesses are better equipped to comply with guidelines than consumers.

Wearables present additional challenges to traditional notions of privacy such as FIPPs.[168] Because many wearables are screenless or do not

158. *Id.*

159. *Id.*

160. *Id.*

161. Cate, Fred H., *The Failure of Fair Information Practice Principles*, CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY, at 343 (2006), https://ssrn.com/abstract=1156972.

162. *Id.*

163. *Id.*

164. *Id.*

165. *Id.*

166. *Id.* at 2.

167. CFPB, *A Summary of Your Rights Under the Fair Credit Reporting Act* (available at https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf) (last visited Apr. 19, 2020).

168. Janice Phaik Lin Goh, *Privacy, Security, and Wearable Technology*, 8 LANDSLIDE 30, 31 (2015).

provide users the ability to interact in a meaningful way, users may have an even more difficult time availing themselves of the notice and choice model.[169] To provide consent, it would likely have to be through an associated app that is located on another device.[170]

F. Food, Drug, and Cosmetic Act

The Food and Drug Administration (FDA) generally has broad authority to regulate products marketed to the public. Unfortunately, it has done little to protect the privacy of people who use wearable mHealth devices.

Under the Food, Drug, and Cosmetic Act (FDCA), a medical device is "any product intended for use in the diagnosis of disease or of the body."[171] The FDCA provides that "device" does not include "a software function that is intended … for maintaining or encouraging a healthy lifestyle and is unrelated to the diagnosis, cure, mitigation, prevention, or treatment of a disease or condition."[172] With technological developments in wearables and mHealth apps, the FDA has clarified that mobile phone applications will be regulated if they are intended: (1) to be used as an accessory to a regulated medical device; or (2) to transform a mobile platform into a regulated medical device.[173]

In the last decade, the FDA has developed a Digital Health Program that, according to the agency, balances "the benefits and risks to patients."[174] The FDA explains it has "focused [the agency's] oversight on mobile medical apps to only those that present *higher risk* to patients, while choosing not to enforce compliance for *lower risk* mobile apps."[175] Likewise, it states it will not focus on "technologies that receive, transmit, store or display data from medical devices," or "products that only promote general wellness."[176] In other words, apps that work with higher risks devices, e.g., implanted devices, would be categorized as "high-risk," whereas an Apple Watch or Fitbit would be a "low-risk" device.

In July 2017, the FDA released its *Digital Health Innovation Action Plan*, again stating the agency does not plan to regulate "low risk general wellness products." The plan explains the agency's direction over the

169. *Id.*

170. *Id.*

171. 21 U.S.C.A. § 321(h).

172. 21 U.S.C.A. § 360j.

173. Durkin, *infra* note 156, at 284.

174. *Digital Health Innovation Action Plan*, U.S. FOOD & DRUG ADMIN. (2017), *at* 2, *available at* https://www.fda.gov/media/106331/download.

175. *Id.* (emphasis added)

176. *Id.* at 3.

coming year to "encourage digital health innovation." The plan mapped out three areas of action: (1) issuing new guidance regarding the regulation of digital health, (2) developing new regulatory approaches to the oversight of digital health, and (3) building expertise on digital health within the agency.[177]

The FDA explains that its hands-off approach is rooted in getting products to consumers quickly and not stifling innovation.[178] The FDA stated, "For the American people to see the full potential of digital health technologies, FDA must lean forward and adapt our processes."[179] As such, the FDA has limited the scope of its regulation to "medical devices," under the FDCA, used in the diagnosis of disease or other conditions, or in the cure, mitigation, or prevention of disease.[180] To determine whether a product is a medical device, the FDA will consider how a manufacturer intends its product to be used.[181] This regulatory scheme creates a loophole between what a manufacturer intends its product to be used for and how it is actually used.[182] According to one critic, "consumer access, self-treatment, the unauthorized practice of medicine, and the actual use [of mHealth apps] have coalesced into a state where technological advancement encourages self-treatment and the unauthorized practice of medicine."[183]

A study led by Lori Andrews, in *Privacy a New Privacy Paradigm*, compared what apps' privacy policies say what they do with the users' information and what they actually do with the information.[184] With large amounts of money being offered by data brokers for sensitive medical data, unscrupulous developers have entered the market to seize on the opportunity.[185] Because medical apps provide users the opportunity for self-

177. Wade Ackerman & Christina Kuhn, *FDA Releases Details and Timelines in Its Digital Health Innovation Action Plan*, COVINGTON (Aug. 3, 2017), https://www.covingtondigitalhealth.com/2017/08/fda-releases-details-and-timelines-in-its-digital-health-innovation-action-plan/.

178. FDA, *supra* note 134, at 2.

179. *Id.*

180. *See* Federal Food, Drug, and Cosmetic Act, Pub. L. No. 75-717, 52 Stat. 1040 (1938) (codified as amended at 21 U.S.C. §§ 301-399) (defining and outlining medical devices intended for human use); *See also* Terence M. Durkin, *Health Data Privacy and Security in the Age of Wearable Tech: Privacy and Security Concerns for the Nflpa and Whoop*, 19 J. HIGH TECH. L. 279, 283 (2019).

181. *See* Vincent J. Roth, *The mHealth Conundrum: Smartphones & Mobile Medical Apps—How Much FDA Medical Device Regulation is Required?*, 15 N.C. J. OF L. & TECH. 359, 364 (2014).

182. *Id.*

183. *Id.* at 365

184. Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 428 (2018).

185. *Id.* at 466.

treatment, a poorly designed app can have deadly consequences. Andrews' study found that 43% of diabetes apps were designed for disease management and 19% allowed the user to calculate insulin doses and the amount of carbohydrates consumed.[186] Thirty-five percent of the bipolar apps examined in the study similarly tracked medications, vitals, or symptoms.[187] Forty-one percent told the user what dose of a drug to take or what other action the user should undertake to treat her condition.[188] Ultimately, the study found that apps offered unproven treatments. Several apps aimed at treating bipolar disorder actually discouraged users from going to the doctor or taking recommended medications, and instead urged users to listen to southing sounds, which were advertised as "Doctor's #1 recommendation for mental illness treatment."[189] Of the apps that were supposed to warn about drug interactions, 67% failed to recognize a potentially fatal interaction.[190] None of the medication tracking apps gave a warning when a tester input a lethal 6000 mg dose of lithium – one of the apps even brought up an advertisement offering to sell the user more lithium.[191] Other studies have shown deficiencies in asthma apps, diabetes apps, and other medical apps.[192]

With wearables having an increasing presence, apps that work with wearables will follow. Without regulation, the apps will continue to have potentially harmful – or even deadly – effects. Self-regulation of the market is not protecting consumers or creating a market conducive to innovation. Legitimate wearable technology, and the mHealth apps based on them, are being forced to compete against free apps that physically endanger users and negatively impact the overall market. Also, if too many consumers have negative experiences with wearables and related apps, they are less likely to use other wearables and apps and would not recommend them. Ultimately, the few bad apples would spoil the bunch.

186. *Id*.
187. *Id*.
188. *Id* at 466-67.
189. *Id.* at 467.
190. *Id.*
191. *Id.*
192. *Id.*

Part IV: Potential for Improving Health Outcomes

A. Precision Medicine

Medical progress is not much different than other forms of progress: it requires learning from one's successes and mistakes. Not having complete information makes it difficult to learn from either. Wearables have the potential to harness technology for medical research that could provide doctors with more complete data sets.[193] In one study of stroke patients, informed consent was obtained from only 39.3% of patients in phase one and 50.6% in phase two.[194] This led to selection bias: the patients that were impaired or seriously ill did not provide written consent.[195] The point is not to dispense with the opt-in consent requirement for medical research, but to identify ways to increase opt-in consent rates. Wearables may be part of the solution.

In 2017, Stanford launched a study of whether a mobile app that uses data from a heart-rate pulse sensor, on the Apple Watch, could identify atrial fibrillation.[196] Atrial fibrillation is an irregular and often rapid heart rate that can increase risk of strokes, heart failure, and other heart-related complications.[197] The condition often remains undiagnosed because many people do not experience symptoms.[198] The virtual study had an unprecedented 400,000 enrolled participants.[199] One key finding of the study was the following: "Comparisons between irregular pulse-detection on Apple Watch and simultaneous electrocardiography patch recordings showed the pulse detection algorithm (indicating a positive tachogram reading) has a 71 percent positive predictive value."[200] Loyd Minor, MD, Dean of Stanford School of Medicine, said, "Atrial fibrillation is just the beginning, as this study opens the door to further research into wearable technologies and how they might be used to prevent disease before it strikes — a key goal of precision health."[201]

193. Uttam Barick, *Harnessing Real World Data From Wearables and Self-Monitoring Devices: Feasibility, Confounders and Ethical Considerations*, 4 MEFANET J. 44 (June 27, 2016).

194. *Id.* at 1453.

195. *Id.*

196. *Apple Heart Study demonstrates ability of wearable technology to detect atrial fibrillation*, STAN. MED. NEWS CTR. (Mar. 16, 2019), https://med.stanford.edu/news/all-news/2019/03/apple-heart-study-demonstrates-ability-of-wearable-technology.html.

197. *Atrial Fibrillation Overview*, MAYO CLINIC, https://www.mayoclinic.org/diseases-conditions/atrial-fibrillation/symptoms-causes/syc-20350624 (last visited Apr. 20, 2020).

198. STAN. MED., *supra* note 176.

199. *Id.*

200. *Id*

201. *Id.*

The FDA defines precision medicine as, "an innovative approach to tailoring disease prevention and treatment that takes into account differences in people's genes, environment, and lifestyles."[202] Precision medicine has been called the optimistic marriage of high-tech and high-touch.[203] Whereas medicine has been traditionally directed towards the general population, wearables create opportunities for continuous health monitoring for individual patients. Wearables might be joined by implantables, ingestibles, and invisibles.[204]

As technology advances, so does security and privacy concerns. Wearables and implantables can be hacked.[205] In 2017, the FDA released a Safety Communication warning that there were 465,000 implanted pacemakers requiring a firmware update to address cybersecurity vulnerabilities.[206] Indeed, mHealth may have the ability to revolutionize healthcare, but if not done correctly, it may also place many lives and livelihoods in jeopardy. Because privacy and security will be crucial in developing trust with consumers, these principles should be a forethought rather than an afterthought. In doing so, more users will opt-in, creating a more complete data set that the medical field can rely on. Nonetheless, this takes trust. As precision medicine takes its first steps, it should keep in mind that trust is fragile and should not be overlooked in favor of convenience.

B. COVID-19

The world is fighting the COVID-19 pandemic.[207] As of September 21, 2021, the John Hopkins Coronavirus Resource Center reported 229,517,471 cases, 4,707,807 deaths, and 223 countries with confirmed cases of COVID-

202. *Precision Medicine*, U.S. FOOD & DRUG ADMIN. (Apr. 2, 2020), https://www.fda.gov/medical-devices/vitro-diagnostics/precision-medicine.

203. *Precision Health*, STAN. MED. (Mar. 5, 2020), https://med.stanford.edu/precisionhealth.html.

204. *See* Chris Van Hoof, *Wearables, Ingestibles, Invisibles: imec at CES 2020*, MEDGADGET (Jan. 10, 2020), https://www.medgadget.com/2020/01/wearables-ingestibles-invisibles-imec-at-ces-2020.html (Ingestibles are swallowed, go into the digestive track, and monitor what a users' body does with food, which provides the ability to give precise prescriptive advice on nutrition. Invisibles are radar-based sensors that are not on one's body, but rather, near it; they track heart rate or respiration rate through sensors on a seat or mattress).

205. Florence Hudson, *Wearables and Medical Interoperability: The Evolving Frontier*, IEEE (Sept. 2018), https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8481273.

206. *Id.*

207. *COVID-19 Dashboard*, JOHN HOPKINS CORONAVIRUS RES. CTR., https://coronavirus.jhu.edu/map.html (last visited Sept. 21, 2021); *see also Number of novel coronavirus (COVID-19) deaths worldwide as of September 20, 2021, by country*, STATISTA, https://www.statista.com/statistics/1093256/novel-coronavirus-2019ncov-deaths-worldwide-by-country/ (last visited Sept. 21, 2021).

19.[208] One of the challenges affecting the medical community's ability to contain the virus is the long incubation period, ranging from 5-14 days.[209] During this time, infected individuals can go without symptoms, which means the person may unknowingly spread the virus.[210]

Wearables have been used to detect symptoms of COVID-19.[211] For example, Cardiogram is an app on Apple Watches that serves as a heart rate monitor. Through its Sleeping BPM function, it can "help users become aware of how their body is responding to symptoms of the flu or other illnesses, including COVID-19."[212] The developers caution that the app is not a replacement for medical diagnostic tests.[213]

On the other hand, there are fears that such monitoring of personal health information could produce a long-term problem for a short-term solution.[214] Historically, during times of emergencies, governments have stripped away social liberties and have not relinquished their emergency powers afterwards.[215] As Edward Snowden states, "the funny thing is [for the government] the emergency never ends; it becomes normalized."[216] There are fears that when this emergency is over, the expanded capabilities and data sets given to businesses and government will be kept and used for small-time criminality, political gain, and maintaining power dynamics.[217] For reasons previously mentioned in this paper, the information collected by wearables provides access to information that a user may be unaware of that could result in discrimination.[218] After the virus is defeated, companies and

208. *Id.*

209. *Id.*

210. *Id*.

211. Mike Peterson, *Apple Watch users can monitor their body's response to COVID-19, flu with Cardiogram app,* APPLEINSIDER (Mar. 19, 2020), https://appleinsider.com/articles/20/03/19/apple-watch-users-can-monitor-their-bodys-response-to-covid-19-flu-with-cardiogram-app.

212. *Id.*

213. *Id.*

214. *Shelter in Place with Shane Smith & Edward Snowden (Full Episode)*, VICE NEWS (Apr. 10, 2020), https://www.youtube.com/watch?time_continue=861&v=k5OAjnveyJo&feature=emb_logo.

215. With the Bush-era warrantless wiretapping program, only part of it was shut down, while the other parts have been repeatedly rolled over; *see* Ellen Nakashima, *Legal memos released on Bush-era justification for warrantless wiretapping*, WASH. POST (Sept. 6, 2014), https://www.washingtonpost.com/world/national-security/legal-memos-released-on-bush-era-justification-for-warrantless-wiretapping/2014/09/05/91b86c52-356d-11e4-9e92-0899b306bbea_story.html.

216. *Id.*

217. *Id.*

218. Singer, s*upra* note 42.

data brokers, may continue to hold this information and use it for financial gains due to the overreaching privacy policies.

Both political parties in the United States have introduced legislation on COVID-19 tracing and tracking, but they remain divided on preemption of state law and private right of action.[219] In May 2020, Senator Roger Wicker introduced the "COVID-19 Consumer Data Protection Act of 2020," but the bill died in committee.[220] Also, Senator Mark Warner introduced the "Public Health Emergency Privacy Act," but it lacks bipartisan support.[221] In all, the political stalemate of Congress coupled with concerns of preemption and a private right of action make the passage of meaningful COVID privacy legislation unlikely. Without such legislation, the current laws do not provide adequate privacy protection for users of advanced technologies that predict diagnosis.

Part V: Conclusion

Traditionally, patients disclosed medical information in a hermetic manner: disclosure was done with just a doctor or other trusted individuals. For the doctor, there are a number of overlapping regulations that protect a patient's medical information.

The calculus changes in light of how wearables and mHealth apps gather, use, and share medical information. Initially, the transaction may seem innocuous, i.e., a user downloads an app to monitor steps, health, and so on. This information may seem harmless. However, by gathering multiple data sets and creating a user profile with a myriad of data points, predictive algorithms and artificial intelligence can try to predict the likely behavior or health status of an individual. These patterns are valuable to insurance companies, employers, and others.

Currently, there is a patchwork of sectoral privacy laws, but a general federal privacy law is lacking. Wearables are not sufficiently covered. Proponents of continuing this hands-off approach argue that regulations would stifle innovation.[222] However, the FTC and FDA have both taken a hands-off approach, which has allowed bad actors to participate. With well-crafted regulations, these bad actors would be removed from the pool and the right kind of innovation would flourish. Regulation would actually

219. Jessica Rich, *How our outdated privacy laws doomed contact-tracing apps*, BROOKINGS (Jan. 28, 2021), https://www.brookings.edu/blog/techtank/2021/01/28/how-our-outdated-privacy-laws-doomed-contact-tracing-apps/.

220. Bradley Arant Boult Cummings LLP, *A Second Chance for the Public Health Emergency Privacy Act*, JDSUPRA (Mar. 2, 2021), https://www.jdsupra.com/legalnews/a-second-chance-for-the-public-health-3911099/.

221. *Id.*

222. Kellog, *supra* note 8.

encourage innovation because legitimate actors would not have to compete with bad actors. Additionally, user trust and confidence would be encouraged, which would result in a larger pool of participants.

Consumer trust is pivotal to increasing user participation. Wearable technology is both exciting and scary. Wearables have the potential to be a truly innovative technology that can facilitate medical progress, help people, and progress society forward. This potential must be weighed against the dangers of the sensitive information that wearables create. For these reasons, trust must be a forethought and not an afterthought.

In September 2014, Tim Cook, CEO of Apple, released a letter addressing privacy concerns.[223] In drafting this letter, Tim Cook created a "gold standard" of self-regulated privacy policy for a company. It argues that privacy should be baked in. It also criticizes companies that collect, share, and use personal data as their business model. To be fair, Apple is in a position to make these assertions because its business model is not selling ads, like Google or Facebook; rather, its business model is to sell devices.[224] On the other hand, Apple's devices host the apps that collect and sell user information, which Apple directly profits from. As of 2018, Apple made $42 billion from App Store downloads.[225] Nevertheless, Apple attempts to foster trust with its consumers by highlighting privacy concerns.

Trust has a direct impact on sales. With COVID-19, there has been a surge in sales of desktop cameras to enable video conferencing.[226] In 2018, Facebook released Portal, an A.I.-powered camera with a video-chat screen.[227] To address privacy concerns, Facebook incorporated a kill switch for the camera, provided a cover for the lens, encrypted video calls, and built the camera's A.I. into the device itself.[228] Yet, despite high demand for desktop cameras during COVID, demand for Facebook's Portal remained low.[229] This is likely attributable to the healthy distrust that users have with

223. Steve Kovach, *Tim Cook Ripped Apart Google's Business Model in 2 Paragraphs*, BUS. INSIDER (Sept. 17, 2020), https://www.businessinsider.com/tim-cook-privacy-letter-2014-9?op=1.

224. *Id.*

225. Chaim Gartenberg, *How Apple Makes Billions of Dollars Selling Services*, THE VERGE (Mar. 20, 2019), https://www.theverge.com/2019/3/20/18273179/apple-icloud-itunes-app-store-music-services-businesses.

226. Bill Thomas, *Where to Buy a Webcam: These Retailers Still Have Stock*, TECHRADAR (Apr. 20, 2020), https://www.techradar.com/news/where-to-buy-a-webcam (last visited Apr. 20, 2020).

227. Mike Isaac, *Facebook's New Gadget Is a Video-Chat Screen With a Camera That Follows You*, N.Y. TIMES (Oct. 8, 2018).

228. *Id.*

229. Jack Kramer et al., *Zuck cancels his Libra moon-landing" –AMC theaters' expiration date. Gilead's corona-cure bet. Facebook's cryptocurrency 180*, ROBINHOOD SNACKS (Apr. 20, 2020) (Podcast).

Facebook. Users are reluctant to purchase a Facebook Portal, which has some solid privacy features, because they do not trust Facebook with their private information. Facebook Portal illustrates the importance of trust.

Because of the sensitivity of medical information, and the long-term and irrevocable nature of disclosing it, medical information should not be commercially sold. There is a wealth of potential in medical innovation as medicine shifts from general care to precision healthcare. Users must have assurances that their medical information will not be sold or result in discrimination. For now, users are largely unaware of the long-term consequences and risks associated with data collection, so they may be willing to trade their privacy for convenience. However, as public sentiment shifts because of growing privacy awareness, such transactions are less likely to occur.

The current sectoral legal framework does not suit the need to ensure innovation of wearables. HIPAA fails for two reasons. First, it only regulates medical information disclosed by a medical provider or someone that does business with them. Therefore, it does not apply to most commercial transactions. Second, there is no private cause of action to enforce it. For a HIPAA violation, a covered entity is fined by the government, but there is no redress for the patient. As for COPPA, its scope is limited to children under the age of 13.

Administrative agencies could regulate wearables and medical information, but they will need more statutory authority to do so. The FTC might make more sense, because the FDA can more likely regulate devices or wearables that are prescribed by a doctor. Whether the FTC has the authority to broadly regulate wearables, outside of deceptive practices, is unclear.

In all, because the relationship between wearables and consumers is particularly exciting but also scary, companies should tread lightly for fear of stifling their long-term goals for short-term gains. The lost trust a user has once their medical information is made public is irreparable and will, ultimately, stifle innovation. To allow good actors to continue to innovate, bad actors must be regulated.

***