Brooklyn Law Review

Volume 82 | Issue 4 Article 6

1-1-2017

Wearables and Personal Health Data: Putting a Premium on Your Privacy

Alexandra Troiano

Wearables and Personal Health Data

PUTTING A PREMIUM ON YOUR PRIVACY

INTRODUCTION

Imagine waking up in the morning—your Fitbit[1] alarm silently buzzing so you don't oversleep. They know you had a restless sleep. You get dressed and decide to walk to work. They know where your office is located. So far, you burned approximately 250 calories. They know you walked 4000 steps. After work, you rush to the gym and get there just in time for your favorite spin class. They know you entered Equinox at 7:20 p.m. After a full day, you haven't reached your goal just yet—15,000 steps. So, after dinner, you decide to take your dog for a long walk until your Fitbit buzzes again, letting you know you reached your goal. You are one step closer to living a healthier lifestyle and they know it. But who are "they?"

Recently, insurance companies have gained greater insight into their policyholders' health habits by incentivizing them to take steps toward a healthier lifestyle through the use of wearable devices and health apps. Mobile health—sometimes referred to as mHealth—applications (apps) have increasingly provided new ways to track and collect personal health data. These apps allow individuals to input personal information including calorie intake, daily movements and exercise, and even vitals.[2] These platforms allow users to view a more comprehensive picture of their personal health and, in turn, take steps toward a healthier lifestyle. In recent years, this technology has expanded to include wearable devices.

Wearable devices, also known as "wearables," are electronic technologies that are incorporated into items of clothing or accessories, such as watches, glasses, and rings.[3]

---

[1] A wearable device worn on an individual's wrist that tracks an individual's daily movements and can act as an alarm clock—silently vibrating at a designated time. *See generally* FITBIT, https://www.fitbit.com/sleep-better [https://perma.cc/A975-5QUV].

[2] Jamie Lynn Flaherty, Note, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 AM. J.L. & MED. 416, 421, 429 (2014).

[3] "Generally, wearable technology will have some form of communications capability and will allow the wearer access to information in real time. Data-input

This technology expands the capabilities of health apps by collecting users' physical activity such as "heart rate, skin temperature, or respiratory rate . . . in real time" and transmitting this collected data into the apps.[4] Wearables increase the efficiency and convenience of tracking biometric data because the device itself can track and store this information while the user simply wears it—even in water and during sleep and exercise.[5] Once the wearable collects data, the information is sent wirelessly to a health app on a smartphone or computer, or sent to the "cloud."[6] Users can then view a complete image of their health by looking at their compiled data on a mobile app via a smartphone or on a computer.

While wearable devices have been commonly used in the medical field,[7] recently there has been a sharp increase in wearables that serve a more functional purpose—to "recreationally track health and fitness levels."[8] For example, a company called Fitbit Inc. sells a line of wearable fitness-tracking wristbands, or "Fitbits,"[9] that track a user's physical activity while wearing the device, including the number of steps taken, distance travelled, and calories burned. The device includes a GPS monitor, a heart rate monitor, and an alarm[10] and can even compile exercise summaries.[11] Fitbit holds the first spot in the wearables market, with Apple Inc. in the number three spot.[12] Fitbit sold 10.9 million devices in 2014

---

capabilities are also a feature of such devices, as is local storage." *Wearable Technology and Wearable Devices Everything You Need to Know*, WEARABLE DEVICES, http://www.wearable devices.com/what-is-a-wearable-device/ [https://perma.cc/J45R-FFKG] (last updated Mar. 26, 2014).

[4] Matthew R. Langley, Note, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 GEO. L.J. 1641, 1644 (2015).

[5] *See id.*

[6] Ruby A. Zefo, *Wearable Devices: Keep Data Privacy in Check,* INFO. WEEK (Aug. 18, 2014), http://www.informationweek.com/mobile/mobile-devices/wearable-devices-keep-data-privacy-in-check/a/d-id/1298085 [https://perma.cc/288C-CNNB]. *PC Mag* defines "cloud computing" as "storing and accessing data and programs over the Internet instead of your computer's hard drive. The cloud is just a metaphor for the Internet." Eric Griffith, *What Is Cloud Computing?*, PC MAG. (May 3, 2016), http://www.pcmag.com/article2/0,2817, 2372163,00.asp.

[7] *See, e.g.*, Spela Kosir, *Wearables in Healthcare*, WT (Apr. 15, 2015), https:// www.wearable-technologies.com/2015/04/wearables-in-healthcare/ [https://perma.cc/2AGX-GA6H].

[8] Langley, *supra* note 4, at 1644.

[9] FITBIT, http://www.fitbit.com/home [https://perma.cc/8RBG-2T8V].

[10] *See Our Technology*, FITBIT, https://www.fitbit.com/technology [https:// perma.cc/87R3-EMG9].

[11] *SmartTrack*, FITBIT, https://www.fitbit.com/smarttrack [https://perma.cc/ 8GYM-46EW].

[12] Jeff Dunn, *Fitbit is Still the Leader In Wearables, but It's Losing Its Grip*, BUSINESS INSIDER (Mar. 7, 2017), http://www.businessinsider.com/fitbit-vs-apple-watch-xiaomi-wearable-sales-chart-2017-3.

and "sold 1.6 million in the first three months of 2015."[13] In the third quarter of 2015 alone, the company sold 4.8 million connected devices and raised $409.3 million in revenue.[14] While Fitbit sales have declined this past year due to interest in other products, such as the Apple Watch or cheaper wearable devices, the company shared its plan to "turn Fitbit into a digital-health company—one that relies less on consumers and focuses on selling to the health-care industry."[15]

Since the release of the original Fitbit, there has been a dramatic increase in wearable technologies and their capabilities.[16] Other types of wearable technology include smartwatches,[17] smart glasses,[18] and smart shirts that track biometric information.[19] According to a recent report by Tractica, a market intelligence firm, global revenue from wearable devices is forecasted to reach $6.3 billion by 2020—a dramatic increase from the "$218 million revenue in 2015."[20] The report also predicts that over 75 million wearable devices will be sold between the years 2014 and 2020.[21]

The market for these devices continues to grow and even employers are implementing wellness programs using these wearables to increase productivity and healthy habits within the workforce. Now, insurance companies offer discounts

---

[13] Brian Dolan, *Fitbit Files for IPO, Sold Nearly 11 Million Fitness Devices in 2014*, MOBIHEALTHNEWS (May 7, 2015), http://www.mobihealthnews.com/43412/fitbit-files-for-ipo-sold-nearly-11-million-fitness-devices-in-2014 [https://perma.cc/M5FJ-U7LW].

[14] Press Release, Fitbit, Fitbit Reports $409M Q315 Revenue; Raises Guidance to $1.77 to $1.80B FY15 Revenue (Nov. 2, 2015), https://investor.fitbit.com/press/press-releases/press-release-details/2015/Fitbit-Reports-409M-Q315-Revenue-Raises-Guidance-to-177-to-180B-FY15-Revenue/default.aspx [https://perma.cc/4LC5-JG7S].

[15] Selina Wang, *Fitbit's Sales Plummet as Device's Popularity Fades*, BLOOMBERG TECHNOLOGY (Feb. 22, 2017), https://www.bloomberg.com/news/articles/2017-02-22/fitbit-s-fourth-quarter-sales-drop-as-device-s-popularity-fades [https://perma.cc/W9TJ-9FVG].

[16] *See generally* Martin Gee, *A Day in the Life of Wearable Tech*, TIME, http://time.com/see-the-wearable-tech-of-the-future/ [https://perma.cc/QV6D-4KGE].

[17] Tyler Biscontini, WEARABLE TECHNOLOGY, Salem Press Encyclopedia of Science, (Jan. 2015) ("Smartwatches mimic the appearance of traditional watches, featuring digital screens that display time and additional information. Most smartwatches pair with a user's smartphone, allowing the user to see messages or calls on the watch that the phone has received. Some smartwatches are even capable of taking pictures, sending messages, and making phone calls.").

[18] *Id.* (Smart glasses "use a translucent material placed in front of one or both eyes to project a screen directly into the user's field of vision. Most smart glasses function by tracking the hand and eye movements of the users and syncing their movements with the projected display. The glasses can function as a global positioning system (GPS), access the Internet, and take hands-free videos and pictures.").

[19] *Id.*

[20] Vera Gruessner, *Wearable Devices Market Expected to Reach $6.3 Billion by 2020*, MHEALTH INTELLIGENCE (Oct. 19, 2015), http://mhealthintelligence.com/news/wearable-devices-market-expected-to-reach-6.3-billion-by-2020 [https://perma.cc/M2H6-W43R].

[21] *Id.*

to policyholders who use Fitbits, or other wearable wristbands, to track and report health information.[22] At first glance, this idea seems like a win-win for insurance companies and policyholders—insurance companies can reduce risk by encouraging healthier habits for their policyholders, and policyholders can receive discounts on their health insurance. Despite this synergy, however, this type of program threatens personal privacy, particularly in the realm of health insurance, because vast amounts of data are being collected and there is a lack of clear regulation controlling the dispersion of this information. Now, not only will health insurance providers gain unrestricted access to an individual's full health profile—which may include information regarding an individual's illnesses or other conditions and influence the premium price or the coverage status, but they will also have access to all of the other information collected by these devices, such as the location of the user at a given time. Even more threatening is the fact that privacy regulations surrounding the collection—as opposed to the dissemination—of this type of information is less than sound, creating opportunities for third parties and hackers to gain access to an individual's personal health information. While laws and regulations "protect" some of this information by requiring companies to implement safeguards and, in some states, to notify individuals of leaks or hacks, these safeguards inadequately protect consumers from other possible dangers.[23]

Due to the increased risks that go hand-in-hand with technological advancements and increased data collection, the United States should adopt new regulations to govern the collection, storage, and dissemination of this information in order to protect consumer privacy. In order to remedy privacy threats posed by the collection and usage of information gathered from wearables and other advancing technology, particularly in the field of insurance, the law should require insurance companies to inform policyholders of exactly what data it collects and exactly how the data is used. More specifically, the United States should adopt mandatory regulations—mirroring that of the General Data Protection Law (GDPR)—that require, rather than merely suggest, data protections for the consumer.

---

[22] *See, e.g.*, Lucas Mearian, *Insurance Company Now Offers Discounts—If You Let It Track Your Fitbit*, COMPUTERWORLD (Apr. 17, 2015), http://www.computerworld.com/article/2911594/insurance-company-now-offers-discounts-if-you-let-it-track-your-fitbit.html [https://perma.cc/9G72-VCUT].

[23] *See infra* Section II.B.

Part I of this note explores the general benefits and consequences of wearables devices. Part II analyzes the current laws that apply to the regulation of data collected by wearables. It also discusses how these laws inadequately address both the larger problem of underregulation of privacy protection in the wearable context and the more specific problem this note seeks to solve: insurance companies' use of wearable devices to track policyholder information. Finally, Part III proposes that the United States adopt new regulations governing data protection generally, modeled after the regulations proposed by the European Commission in 2012. The United States should adopt regulations that impose safeguards on all personal data collection and processing in order to protect consumers from the pervasiveness of electronic devices. These regulations should, however, also leave room for innovation and progress.

I. THE GENERAL BENEFITS AND CONCERNS OF WEARABLE DEVICE USAGE

Health apps and wearables introduce significant benefits in terms of general health and personal convenience. Wearables, especially those designed to track physical movement and sleeping patterns, encourage healthy lifestyles. Problematically, however, wearables also collect and store personal health information that may not be safeguarded effectively.[24]

A. The Benefits of Wearables

Health apps have numerous social benefits as a result of the convergence between technology and healthcare. This technology offers a form of "healthcare at a lower cost," increased patient control over personal healthcare, and "easier and more immediate access" to healthcare information.[25] Wearables—which allow a user to more closely track movement and vitals—add to these benefits because they provide more accurate tracking capabilities and quantify large amounts of personal data: "The combination of ubiquitous use and connectivity . . . together with Big Data and data mining plays

---

[24] *See infra* Section I.B.

[25] *Opinion of the European Data Protection Supervisor on Mobile Health, Reconciling Technological Innovation with Data Protection*, 1/2015, at 3 (May 21, 2015), https://edps.europa.eu/sites/edp/files/publication/15-05-21_mhealth_en_0.pdf [https://perma.cc/3SQE-3E7M].

a crucial role in mHealth, building a digital image of each of us (so-called *quantified self*)."[26]

Fitness trackers such as Fitbits encourage healthy behavior through their tracking capabilities.[27] Fitbits—and their health app counterparts—allow users to track their sleep patterns and physical activity, analyze this data, and set personal goals for movement and exercise throughout the day. For example, with a Fitbit, a user can turn on silent alarms, enter their calorie intake, and monitor logged health data "such as blood pressure, heart rate, glucose readings, and allergy severity."[28]

Health apps and wearables have the ability to promote healthy habits and cut healthcare costs because they provide easy access to health resources and encourage users to live a healthier lifestyle—even for those with more serious or chronic conditions than an average user.[29] This technology may reduce hospital readmissions because patients are able to more effectively self-monitor their own health.[30] For example, apps such as mySugr Diabetes Logbook allow individuals with diabetes to monitor their glucose levels by tracking their sugar intake and analyzing the inputted information.[31] The app will alert the user to changes in health and can even provide the user's doctor with reports.[32] The accuracy and convenience of these apps ultimately increase the likelihood that users will seek preventative medical care and thus reduce hospital admissions and readmissions.

Users of wearable devices likely utilize their app counterparts because of convenience: "[wearables are] increasing the popularity of apps over traditional web browsing experiences."[33] Moreover, "[b]ecause wearable devices have smaller screens and more intuitive interfaces, users will begin

---

[26] *Id.* at 3. (citing Kelvin Kelly, founder of *Wired*, who established the platform *quantifiedself.com* with journalist Gary Wolf, and introduced the concept to a broader audience).

[27] *See* Joanne Kaufman, *I Have Miles to Go Before I Sleep: My Electronic Pal Fitbit Urges Me on to Greater Lengths . . . and Heights*, WALL ST. J. (Apr. 16, 2014), http://www.wsj.com/articles/SB10001424052702303603904579496123006797640.

[28] Jill Duffy, *Fitbit Charge*, PC MAG. (Dec. 6, 2014), http://www.pcmag.com/article2/0,2817,2473164,00.asp.

[29] Flaherty, *supra* note 2, at 420. The availability of these resources promotes healthier lifestyles and may "enabl[e] users to better manage chronic conditions." *Id.*

[30] *Id.*

[31] MYSUGR, https://mysugr.com/apps/ [https://perma.cc/HE88-5TWU].

[32] *How to Use MySugr Logbook Reports*, MYSUGR (Nov. 4, 2015), https://mysugr.com/how-to-use-mysugr-logbook-reports/ [https://perma.cc/Y4BK-Q8VX].

[33] Larry Alton, *How Wearable Tech Could Spark a New Privacy Revolution*, CRUNCH NETWORK (Sept. 12, 2015), http://techcrunch.com/2015/09/12/how-wearable-tech-could-spark-a-new-privacy-revolution/ [https://perma.cc/VZC7-DMS5].

relying on apps over any other type of function or service."[34] The app counterparts allow users to view a complete health profile in one place—either on their smartphone or on their computer—so users can view their health profile almost anywhere at anytime.

Wearable technology is not only limited to wristband trackers like Fitbits, but also includes other technology with tracking capabilities. One form of this sophisticated technology is used in the sports arena. Professional sports teams use wearable technology to track athletes' health information and statistics.[35] For example, the NFL partnered with Zebra technologies to "collect data generated by radio-frequency identification transmitters in the shoulder pads of the players."[36]

> The sensors capture precise location measurements in real time during games, reportedly at a rate of about 25 times per second, which translates into location tracking of every player within a margin of error of about six inches for the duration of the entire game. . . . Zebra's MotionWorks server software processes the information, and sends a variety of stats out to NFL's broadcast partners, as well as for use by the league's other partners, and in its NFL app and XboxOne.[37]

Several other leagues employ similar programs in order to "enhance fan engagement[,] . . . reduce injuries and maximize training."[38] These programs allow players and coaches to benefit from an in-depth analysis of performance, which can help monitor player fatigue and prevent injury.[39] These statistics have generated creative uses too: the statistical information can be used in videogames, thereby providing fans with real information and a more realistic experience.

Wearable devices also provide specific benefits depending on the environment in which they are used. In the workplace, wearables, aside from uses that increase productivity and efficiency,[40] can encourage employees to live a healthier lifestyle,

---

[34] *Id.*

[35] Brian Socolow, *Wearable Tech Will Change Pro Sports—and Sports Law*, LAW360 (Sept. 17, 2015), http://www.law360.com/articles/701415/wearable-tech-will-change-pro-sports-and-sports-law [https://perma.cc/2V2P-M7CM].

[36] *Id.*

[37] *Id.*

[38] *Id.* For example, the NBA uses technology to "track and analyze player performance." A sensor in the player's jersey tracks the player's speed, movement, and position. *Id.* The data collected and the "hardware and software together allow teams to look at biomedical data, including impact forces, turn rates and orientation, as well as tactical information, such as two-dimensional animations of the play in real time or post-practice." *Id.*

[39] *Id.*

[40] Wearable devices can serve functions outside of health and fitness tracking capabilities. For example,

thereby reducing health-related costs.[41] Some employers already take advantage of this benefit.[42] For example, Appirio—an information technology consulting company[43]—implemented a corporate wellness program in which it distributed 400 Fitbits to employees throughout the company.[44] Employees chose to share some or all of the data collected on the device and the company received a 5% discount from its insurer, Anthem, after providing Anthem with the collected data.[45] All parties received a benefit from this program: the employees got free Fitbits, the company received a discount on its insurance, and the insurance company received the benefit that its policyholders were presumably living healthier lifestyles, thereby reducing overall risk and cost.[46] Numerous other employers have also implemented corporate wellness programs utilizing the Fitbit. Tokyo Electron—a Japanese company that manufactures semiconductors[47]—estimated that it would be paying $3200 per employee per year if it had not implemented a wellness program using the Fitbit.[48] Also, Tokyo Electron's

---

> [i]n logistics and delivery, . . . parcel handlers may wear scanning devices that offer "tactile feedback"—a short buzzing sensation—if the handler misplaces a package. In the aircraft industry, heads-up displays ("HUDs") increase flight safety by improving the situational awareness of pilots during bad weather conditions and night flights. And across industries, employees who are constantly on their feet may be equipped with watches that allow them to interface with a screen while remaining hands-free.

Christine E. Lyon, *Going to the Heart of Workplace Health Programs and Apps*, LAW360 (Sept. 18, 2015), http://www.law360.com/articles/704029/going-to-the-heart-of-workplace-health-programs-and-apps [https://perma.cc/8G5N-AV9L].

[41] *Id.*

[42] In February 2014, Bates College implemented an employee wellness program in which they distributed Fitbits to participating employees. James A. Martin, *Pros and Cons of Using Fitness Trackers for Employee Wellness*, CIO (Mar. 24, 2014), http://www.cio.com/article/2377723/it-strategy/pros-and-cons-of-using-fitness-trackers-for-employee-wellness.html [https://perma.cc/5PBQ-UJH3]. The college implemented an eight-week competition among participating employees to encourage healthy living. *Id.* "Employee wellness programs are the norm today. Nearly 80 percent of organizations with more than 1,000 employees and 44 percent of firms with between 50 and 999 employees provide them, according to a 2012 survey by Automatic Data Processing." *Id.*

[43] APPIRIO, https://appirio.com/about/company-overview [https://perma.cc/FXP3-S6JN].

[44] Jonah Comstock, *Employer Gets $280K Insurance Discount for Using Fitbits*, MOBIHEALTHNEWS (July 15, 2014), http://mobihealthnews.com/34847/employer-gets-280k-insurance-discount-for-using-fitbits/ [https://perma.cc/M49D-3XCQ].

[45] *Id.*

[46] *See id.*

[47] *See Business Portfolio*, TOKYO ELECTRON, http://www.tel.com/about/portfolio/index.htm [https://perma.cc/33FH-NSEY].

[48] The company estimates that it would pay $15,000 per employee rather than $11,800 per employee. Parmy Olson, *Fitbit's Game Plan for Making Your Company Healthy*, FORBES (Jan. 8, 2016), http://www.forbes.com/sites/parmyolson/2016/01/08/fitbit-wearables-corporate-wellness/#796975d4527a [https://perma.cc/X339-VRTP].

number of annual claims dropped from 11% in 2008 to 5% in 2016 due to this program.[49]

Insurance companies have also recognized these adaptable benefits of wearables and found a way to integrate wearables into individual policyholder plans independent of an employer program.[50] John Hancock, a health insurance company, now offers discounts to policyholders who use Fitbit wristbands to track and report their health information,[51] and other insurance companies are following in its footsteps.[52] Insurance companies can greatly benefit from personal health information gathered through wearables in order to better assess policyholder health profiles. In general, insurance companies use risk assessment in order to calculate premium rates[53] for their policyholders.[54] Premium rates are calculated based on mortality, or life expectancy, and the rate of interest from investment of premiums.[55] In terms of life insurance, a person's lifestyle will affect a user's premium. For example, if a user participates in "dangerous hobbies like skydiving, mountain climbing or motorcycle riding," her premium will likely increase.[56] Similarly, and more importantly in this context, a user's personal health status will greatly affect that user's premium because it provides a good indication of future cost for the insurance company.[57] In other words, the worse a person's health status or condition is, the higher the premium because the insurance company must account for the greater risk this individual presents.

In this way, data collected from wearable devices and the accessibility of this information through the devices' mobile app counterparts allow insurance companies to easily assess their

---

[49] *Id.*

[50] Mearian, *supra* note 22; *see also* Jonah Comstock, *One More Industry That Wants Your Fitbit Data: Life Insurance*, MOBIHEALTHNEWS (Apr. 8, 2015), http://mobihealthnews.com/42210/one-more-industry-that-wants-your-health-data-life-insurance/ [https://perma.cc/8MGK-GHBV] (discussing how health insurance companies have teamed up with wearable companies to implement wellness programs).

[51] Tara Siegel Bernard, *Giving Out Private Data for Discount in Insurance*, N.Y. TIMES (Apr. 8, 2015), http://www.nytimes.com/2015/04/08/your-money/giving-out-private-data-for-discount-in-insurance.html?_r=0 [https://perma.cc/XB5P-9Z49].

[52] *See infra* Section II.A.

[53] The cost for insurance per individual.

[54] *Finding Insurance Insider Information: How Insurance Companies Measure Risk*, INSURANCE COS.COM, http://www.insurancecompanies.com/insider-information-how-insurance-companies-measure-risk/ [https://perma.cc/6HGE-MM2H].

[55] *Life Insurance Resource Center*: *How the Cost of Life Insurance Is Determined*, N.Y. DEP'T OF FIN. SERVS., www.dfs.ny.gov/consumer/cli_h_cost.htm [https://perma.cc/2LNU-PC8D].

[56] *Finding Insurance Insider Information: How Insurance Companies Measure Risk*, *supra* note 54.

[57] *Id.*

policyholders and determine that future cost. This approach appears innovative, efficient, and fascinating, but there are costs to this type of monitoring by insurance companies.

B. The Concerns of Wearables: Information Dissemination and Data Protection

There are three major concerns that arise with the increasing use of wearables: (1) the lack of safeguards protecting personal health information, (2) the sharing of this data to third parties, and (3) the threat of hackers obtaining this information. In all apps, but in health apps particularly, these concerns are more serious due to the breadth and sensitivity of the shared information. Like other apps, health apps collect data that is manually inputted by the user (i.e., information that the device does not necessarily track itself) and automatically collect (e.g., purchase history), and share this information with third parties such as advertisers and data-collection agencies.[58] But health apps also store personally identifiable information such as heart rate, calories burned, and sleep patterns. Moreover, the sensitive information collected is subject to theft by hackers.[59] Now, as the use of wearables grows, privacy concerns surrounding the use of these devices only expand. As companies increasingly use consumer data in new and different ways, consumers face new types of privacy threats.

The first major concern involves the *type* of data collected. Many argue that health data is the most private form of data that exists.[60] Fitbit and other wearable devices track physical movement, location, heart rate, dietary habits, and other personal health information.[61] While users voluntarily input some data, they are likely unaware of other data that is being collected.[62] For example, a user may expect that their

---

[58] *See infra* notes 71–77 and accompanying text.

[59] Emily Field, *Biggest Privacy Problems in Fitness Trackers Still to Come*, LAW360 (Aug. 19, 2015), http://www.law360.com/articles/686145/biggest-privacy-problems-in-fitness-trackers-still-to-come [https://perma.cc/SPN8-9JTW].

[60] *See* Kelsey Munro, *Data Collection: Wearable Fitness Device Information Tracking Your Life*, SYDNEY MORNING HERALD (Apr. 18, 2015), http://www.smh.com.au/digital-life/digital-life-news/data-collection-wearable-fitness-device-information-tracking-your-life-20150416-1mmzbq.html [https://perma.cc/R9WX-CH8W] (quoting David Vaile from the Cyberspace Law and Policy Community at the University of New South Wales, Sydney, who states, "[h]ealth data is the most sensitive of personal information").

[61] *See supra* Introduction.

[62] "[A] user might assume that a fitness tracker will track number of steps, heart rate, distance of a run, calories burned, and sleep patterns. But the user may not anticipate that . . . many devices collect a great deal of other data." Randi W. Singer &

wearable collects information such as how many steps the user takes or his or her sleeping pattern. But, a user may not be aware that the wearable may be collecting other information, such as "precise location data."[63] Also, mobile apps are "installed on a device, and often running in the background,"[64] meaning that a user can exit out of an app without shutting down the program and then resume using the app where they left off at a later point in time.[65] As a result of this, apps *constantly* collect information about a user.[66]

The second major concern is *where* the information being collected by wearable devices ends up. This information can either be shared voluntarily or be obtained illegally. With regard to the voluntary sharing of data, many companies sell data obtained through their apps to third parties. Information is sold to advertisers to use for "personally targeted ads,"[67] which many users might expect. Or, the data collected may be shared with insurance companies, financial institutions, and employers.[68] In 2014, the Federal Trade Commission (FTC)—the nation's consumer protection agency—conducted a study of twelve mHealth and fitness apps and found that user information was sent to seventy-six third-party companies.[69] The information sold to third parties included "[d]evice information; [c]onsumer specific identifiers; [u]nique device IDs capable of allowing 3rd parties to track users' devices across apps; . . . and [c]onsumer information such as exercise routine, dietary habits, and symptom searches."[70] The Privacy Rights Clearinghouse (PRC)—a nonprofit organization dedicated to protecting consumer privacy[71]—also conducted a study that analyzed user

---

Adrian J. Perry, *Wearables: The Well-Dressed Privacy Policy*, 27 INTELLECTUAL PROP. & TECH. L.J. 24, 24 (2015) (footnote omitted).

[63] *Id.*

[64] Alton, *supra* note 33.

[65] *See id.*

[66] *Id.*

[67] *Id.*

[68] Field, *supra* note 59.

[69] FED. TRADE COMM'N, CONSUMER GENERATED AND CONTROLLED HEALTH DATA (2014), https://www.ftc.gov/system/files/documents/public_events/195411/consumer-health-data-webcast-slides.pdf [https://perma.cc/FV8S-6L7P].

[70] *Id*; *see* Kristen Lee, *Wearable Health Technology and HIPAA: What Is and Isn't Covered*, TECH TARGET (July 2015), http://searchhealthit.techtarget.com/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered [https://perma.cc/CN3Z-XM8A].

[71] *About the Privacy Rights Clearinghouse*, PRIVACYRIGHTS.ORG, https://www.privacyrights.org/about [https://perma.cc/92YY-ADNL]. The Privacy Rights Clearinghouse is a nonprofit organization dedicated to educating consumers and advocating for consumer rights. PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/ [https://perma.cc/TXM6-VSHJ].

privacy in health and fitness apps.[72] The PRC concluded that "information privacy is not currently a priority for developers of mobile health and fitness applications."[73] The PRC study highlighted the main issues regarding privacy risks: the collection of data by advertisers, the collection of data by third party analytics, and unencrypted network connections—which lead to the threat of hackers.[74]

The third major concern is the vulnerability to hackers: "Any device that has the ability to store data (i.e., iPod, MP3, tablet, etc.) also has the ability to connect to a computer and, thus, creates the potential for stolen data."[75] Unencrypted network connections—connections not protected by a password—only heighten this risk. According to the PRC study, "only 53% of the free apps and 44% of the paid apps" transmitted personally identifiable information (e.g., "name, email address, address, geo-location, etc.") using encryption or password-protection.[76] While theft of any one piece of this information can be damaging to a user, a real threat exists when hackers take advantage of the amount of information stored in wearables and engage in full identity theft. FTC Chairwoman Edith Ramirez emphasized the danger of this due to a lack of data security: "identity theft . . . has been the FTC's top complaint for the last 14 years. As the sheer volume of consumer data grows, this issue will only take on added importance."[77]

There are numerous other risks—both foreseeable and unforeseeable—that go hand-in-hand with increased capabilities in these types of technology, such as dangers that result from a hacker's ability to identify a user's location. In an FTC report released in January 2015 entitled "Internet of Things: Privacy & Security in a Connected World" (the IoT Report) the FTC noted that "unauthorized access to data collected by fitness and other devices that track consumers' location over time could endanger consumers' physical safety. Another possibility is

---

[72] *See* LINDA ACKERMAN, PRIVACY RIGHTS CLEARINGHOUSE, MOBILE HEALTH AND FITNESS APPLICATIONS AND INFORMATION PRIVACY: REPORT TO CALIFORNIA CONSUMER PROTECTION FOUNDATION 3 (2013), https://www.privacyrights.org/mobile-medical-apps-privacy-consumer-report.pdf [https://perma.cc/EK56-65YG].

[73] *Id.* at 22.

[74] *Id.* at 21.

[75] Lorri Freifeld, *Wearables at Work*, TRAINING MAG., https://trainingmag.com/trgmag-article/wearables-work [https://perma.cc/8575-SK3N].

[76] ACKERMAN, *supra* note 72, at 19–20 (providing that 43% of the twenty-three free apps analyzed sold data to advertisers, while only one of twenty paid apps analyzed sold to advertisers).

[77] Edith Ramirez, Chairwoman, Fed. Trade Comm'n, Address at the Media Institute (May 8, 2014), https://www.ftc.gov/system/files/documents/public_statements/308421/140508mediainstitute.pdf [https://perma.cc/WH9Z-2PBQ].

that a thief could remotely access data about energy usage from smart meters to determine whether a homeowner is away from home."[78] This information in the hands of a criminal hacker could lead to harm to the person, property, or both.

While consumers generally view some forms of data collection and usage as harmless (e.g., third party advertisers who collect information for marketing purposes), other forms of this data collection can have more serious implications. As mentioned above, the collection of this data can have different implications in the hands of employers, insurance providers, or financial institutions. In the IoT Report, the FTC summarized its findings after conducting numerous workshops.[79] In one of these workshops, Scott Peppet, a professor at the University of Colorado Law School, addressed the new direction wearable companies are heading regarding data collection: "Where are they heading with the data? They are heading in a different direction largely, although I'm sure advertising will also play a role, they are heading towards really core economics or economic functions. Things like credit worthiness, insurance, employability, and the revelation of consumer preferences."[80] Paul Bond of Reed Smith LLP highlighted this same issue and stated that the possibility of hackers is not "just a vague concern. This information is used for stalking, assault and—at some time, with respect to health information—this is information that could be very interesting to potential employers, insurers, people giving you credit."[81] Professor Peppet highlighted that insurance companies can receive an "incredibly detailed and rich picture" of a policyholder based on data collected from wearables and that they can price insurance premiums based on this data.[82] So, while data

---

[78] FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 13 (2015).

[79] 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, 33–34 (2016). *See infra* Section II.B.3.

[80] Transcript of Federal Trade Commission, Internet of Things Workshop at 169 (Nov. 19, 2013).

[81] Field, *supra* note 59.

[82] Peppet stated,

> Why? Because these data coming off of sensors are incredibly high quality. I can paint an incredibly detailed and rich picture of who you are based on your Fitbit data or any of this other fitness and health data. And that data is so high quality that I can do things like price insurance premiums or I could probably evaluate your credit score incredibly accurately. The data are going to move towards those economic purposes because they are so useful for that.

Transcript of Federal Trade Commission, Internet of Things Workshop, *supra* note 80, at 169.

collection and its risks may seem daunting, in general, the risks become particularly heightened in the context of wearable devices and their new uses in the economy.

II. PRIVACY ISSUES RELATING TO INSURANCE COMPANIES' NEW RELATIONSHIP WITH POLICYHOLDERS

Wearable devices, generally, are not explicitly regulated by a federal statute. As shown below, information gathered by wearable devices may fall under certain legal frameworks depending on who is collecting that information and how the collecting entity uses the information. This creates two major problems: (1) the sharing of information between parties (particularly where insurance companies gather this type of information and use it to deny coverage or raise premiums) and, more broadly, (2) the lack of regulations governing wearable devices.

A. The John Hancock Program and Its Legal Problems

The use of wearable devices within the context of insurance companies has its own particular benefits, but also its own downfalls. In April 2015, John Hancock announced its partnership with Vitality, "a service provider that integrates wellness benefits with life insurance," to offer discounts of up to 15% to policyholders who opt to wear internet-connected Fitbit devices to track their exercise.[83] John Hancock provides free Fitbits to policyholders, and the Fitbit tracks activities that can earn policyholders points.[84] The program allows the policyholders to receive discounts, gift cards, and discounted hotel stays and airline fares in exchange for earning points for physical activity, doctor visits, and participation in athletic events.[85] Michael Doughty, president of John Hancock Insurance, believes the program will allow policyholders to "connect their financial well-being to their long-term health."[86] Other insurance companies have since implemented similar incentive programs.[87] Oscar, a small insurance company, offered

---

[83] Mearian, *supra* note 22; *see* Bernard, *supra* note 51 (discussing how the John Hancock program works); Comstock, *supra* note 44.

[84] Comstock, *supra* note 44.

[85] Mearian, *supra* note 22.

[86] *Id.*

[87] One large insurance company, Cigna, offers Fitbits or Misfits (another wristband wearable device) to consumers at a discounted price. Mara Lee, *Insurers Offer Cash, Discounts for Fitness Trackers*, HARTFORD COURANT (Sept. 27, 2016), http://www.courant.com/business/hc-aetna-apple-watch-20160927-story.html. The company

policyholders a free Misfit—a wristband fitness tracker—and one dollar for each day they reached their personal goals.[88] Now, members can simply use any fitness tracker that uses Apple HealthKit—a mobile app—to track steps and receive their dollar-per-day discount.[89]

These programs drastically change the way in which insurance companies operate. For those who participate in the program, pricing will no longer be based "on a detailed but static snapshot of a person's medical status," but rather on an individual's health data that wearables collect on a continuous basis.[90] It also changes the insurance company into "less of a passive vehicle that pays the bills if something happens, into a more active vehicle to get people to lower their risk."[91]

The program has many benefits—the most obvious being the insurance company's role in "proactively encourag[ing] healthy behaviors" to allow policyholders' insurance payments to pay out over their lifetimes.[92] In addition to the various incentives given to consumers, these programs generally incentivize policyholders to set health goals and take active

---

offers discounts on premiums and cash incentives for policyholders who partake in their health coaching programs, which involve the use of wearables. Catherine Ho, *Health Insurers Take Steps to Fold Fitness Trackers into Business*, SAN FRANCISCO CHRONICLE (Feb. 5, 2017), http://www.sfchronicle.com/business/article/Health-insurers-take-steps-to-fold-fitness-10907560.php [https://perma.cc/SN89-NMAW]. Other insurance companies offer similar discounts to policyholders and employers involved in employee wellness programs including Humana, United Healthcare, and Health Care Service Corporation. Brian Eastwood, *How Wearing Fitness Tracker Can Lower Your Insurance*, TOM'S GUIDE (July 28, 2016), http://www.tomsguide.com/us/fitness-trackers-insurance,news-23053.html [https://perma.cc/U9VX-YF5M].

[88] Steven Bertoni, *Oscar Health Using Misfit Wearables to Reward Fit Customers*, FORBES (Dec. 8, 2014), http://www.forbes.com/sites/stevenbertoni/2014/12/08/oscar-health-using-misfit-wearables-to-reward-fit-customers/#696d71da2574 [https://perma.cc/FQH9-87P2]; *see* OSCAR, IT'S A FITNESS TRACKER. AND IT'S FREE FOR OSCAR MEMBERS, https://d3ul0st9g52g6o.cloudfront.net/All/All/info/MisfitOverview.pdf?1425958173 [https://perma.cc/C8KC-86BD].

[89] Jonah Comstock, *MHN 2016: For Oscar, Step Tracking Is About Member Engagement, Not Just Health*, MOBIHEALTHNEWS (June 15, 2016), http://www.mobihealthnews.com/content/mhn-2016-oscar-step-tracking-about-member-engagement-not-just-health [https://perma.cc/6HF9-8GMA]. Policyholders can receive up to $100 per year in the form of an Amazon gift card. *Id.*

[90] Bernard, *supra* note 51. John Hancock, in a news release, described the potential savings: "For example, a 45 year old couple (of average heath) buying Protection UL with Vitality life insurance policies of $500,000 each could potentially save more than $25,000 on their premiums by the time they reach 85, with additional savings if they live longer, assuming they reach gold status in all years." *John Hancock Introduces a Whole New Approach to Life Insurance in the U.S. That Rewards Customers for Healthy Living*, PR NEWSWIRE (Apr. 8, 2015), http://www.prnewswire.com/news-releases/john-hancock-introduces-a-whole-new-approach-to-life-insurance-in-the-us-that-rewards-customers-for-healthy-living-300062461.html [https://perma.cc/5DDU-N7UG].

[91] Comstock, *supra* note 44.

[92] *Id.*

steps toward achieving those goals.[93] Participation in the program gives policyholders an opportunity to potentially "save more than $25,000 on their premiums by the time they reach 85."[94] The program also raises several concerns, however, with regard to policyholder privacy. Like other insurance companies that use incentive programs, John Hancock now has access to policyholders' day-to-day behaviors and exercise habits and can even tell the moment policyholders arrive at their local gyms.[95] According to John Hancock, the collected information will not be sold to third parties, but the aggregate data "could be used to inform the development of new insurance products."[96]

This highlights a problem specific to insurance companies and their relationship to policyholders. Typically, when applying for individual life insurance, consumers are required to get a medical evaluation by the insurer.[97] In many cases, a medical technician visits the policyholder's home to collect vital statistics as well as blood and urine samples.[98] But a life insurer typically does not have access to day-to-day behavior.[99] Now, these tracking capabilities—which may someday include the ability to diagnose illnesses—present the possibility that insurers will use information gathered from Fitbits (or other wearables) to deny coverage or increase rates for consumers.[100]

Professor Peppet explained that sensor data, the type of data collected from wearables, is "incredibly hard to anonymize."[101] This means that insurance companies can likely

---

[93] Mearian, *supra* note 22.

[94] *Id.*

[95] *See* Bernard, *supra* note 51.

[96] *Id.*

[97] Rachel Emma Silverman, *Need to Know: Life Insurance 101*, WALL ST. J. (Oct. 15, 2011), http://www.wsj.com/articles/SB10001424052970203633104576625394255572996.

[98] *Id.*

[99] Bernard highlights this exact issue, stating:

> Of course, buying any life insurance policy requires customers to share detailed medical histories upfront. But consumers participating in the Vitality program must be comfortable providing enough information continuously to meet certain thresholds that will convert into worthwhile savings. That might include the frequency of workouts, reporting a physical exam or answering sensitive personal questions: During the last 30 days, how often did you feel so nervous that nothing could calm you down? Hopeless? Depressed?

Bernard, *supra* note 51.

[100] *See* Andrew Boyd, *Could Fitbit Data Be Used to Deny Health Coverage?*, U.S. NEWS & WORLD REP. (Feb. 17, 2017), http://www.usnews.com/news/national-news/articles/2017-02-17/could-fitbit-data-be-used-to-deny-health-insurance-coverage [https://perma.cc/AM5P-2TNQ].

[101] Professor Peppet states,

identify an individual simply from information collected from their wearable.[102] Professor Peppet also highlighted the lack of transparency in the privacy policies of wearable devices: "[I]t is just striking, when you go through the consumer experience, how not salient it is that you are now about to generate a massive amount of new, incredibly high value data that you've never seen before."[103] This raises the issue of consent. How can a consumer consent to giving away personal information if the consumer is unaware of the information being offered?[104]

Finally, the Fitbit's ability to track a policyholder's location presents a very real danger, one that most users would likely find daunting. Location data can reveal where policyholders go to the gym or where they are riding their bikes, but it can also track where they sleep at night, where they go during the day, and when they go to the restroom—which may indicate particular health problems. This can present a problem if a policyholder wears the device around the clock because the location tracking may reveal patterns that would suggest health conditions or personal circumstances that the policyholders "would reasonably expect to be kept private."[105] These particular threats are inadequately addressed by the current regulations surrounding both wearable devices and privacy more generally.

B. The Inadequacies of the Current Regulations Governing Health Apps and Wearables

Currently, there is no federal statute governing privacy in consumer wearables.[106] It is also unclear what regulations apply to this type of relationship between insurance companies, Fitbit, and consumers. There are, however, other laws and regulations governing personal data in particular fields, such as the Health Insurance Portability and Accountability Act

---

> It is just very unlikely that you and I have similar Fitbit data coming off of our Fitbits. Why? Because I move completely differently than you do. Ira Hunt, who is the CIO of the CIA said you can be 100 percent identified, as an individual, by your Fibit data. Why? Because no two persons' gaits or ways of moving are the same. We can almost always figure out who you are based on that kind of incredibly rich detail.

Transcript of Federal Trade Commission, Internet of Things Workshop, *supra* note 80, at 170–71.

[102] *Id.*

[103] *Id.* at 171–72.

[104] *See infra* Section II.B.1.

[105] Lyon, *supra* note 40, at 10.

[106] Langley, *supra* note 4, at 1642.

(HIPAA) that governs patient health data. Government agencies, including the U.S. Department of Health and Human Services (HHS), the Food and Drug Administration, and the Federal Trade Commission, generally play some role in protecting consumers in the context of wearable devices and health apps. Nevertheless, these agencies, and any promulgated regulations, inadequately protect policyholders who participate in the Hancock Program and consumers who will ultimately participate in similar programs in the future.

1. U.S. Department of Health and Human Services

The U.S. Department of Health and Human Services oversees the most relevant regulation regarding individuals' healthcare information: HIPAA. Congress passed HIPAA to protect individuals, to increase portability when individuals change jobs, and to combat waste and fraud.[107] Under HIPAA, covered entities, which include healthcare providers (doctors, clinics), health plans (insurance companies, Health Maintenance Organizations), and healthcare clearinghouses[108] and their business associates[109] are required to protect "individually identifiable health information," otherwise known as "protected health information" (PHI) under the statute.[110] "Individually identifiable health information" includes information related to "the individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to

---

[107] *See Employee Benefits Security Administration*, U.S. DEP'T OF LABOR, https://www.dol.gov/agencies/ebsa/about-ebsa/our-activities/resource-center/fact-sheets/hipaa [https://perma.cc/RCD5-B7EL]; *see also Health Information Privacy*, HHS.GOV, http://www.hhs.gov/hipaa/index.html [https://perma.cc/Q9JT-9EL5].

[108] *Covered Entities and Business Associates*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html [https://perma.cc/QW7T-5Y6J].

[109] A business associate is defined as:

> a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A member of the covered entity's workforce is not a business associate. A covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity. The Privacy Rule lists some of the functions or activities, as well as the particular services, that make a person or entity a business associate, if the activity or service involves the use or disclosure of protected health information.

Business Associates, HHS.GOV, http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/index.html [https://perma.cc/628X-CNTY].

[110] *Summary of the HIPAA Privacy Rule*, HHS.GOV, http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html [https://perma.cc/FPL9-H68X].

the individual."[111] For example, this includes a person's "name, address, birth date, [and] Social Security Number."[112]

The HIPAA Privacy Rule[113] was enacted in response to the "rapid evolution of health information systems" as a result of HIPAA.[114] HIPAA established efficient means for healthcare institutions to transmit information electronically.[115] An increase in the avenues of transferability of PHI created a fear of misuse of that information and an increase in the danger of harmful disclosures.[116] The Privacy Rule responded to "the challenges to the confidentiality of health information presented by the increasing complexity of the health care industry, and by advances in the health information systems technology and communications."[117] Specifically, the Privacy Rule "sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections."[118]

Generally, HIPAA does not cover health and fitness apps. But apps may be forced to comply with HIPAA where they interact with health insurance companies or doctors.[119] According to HIPAA, only "covered entities" and "protected health information" are subject to the privacy requirements. Since they are not included in the definition of "covered entities," most mHealth apps and wearables do not fall subject to HIPAA's regulations. But a health app will fall under HIPAA if a covered entity uses the software.[120] For example, a

---

[111] U.S. DEP'T OF HEALTH & HUMAN SERVS., SUMMARY OF THE HIPAA PRIVACY RULE 4 (2003), https://www.hhs.gov/sites/default/files/privacysummary.pdf?language=es.l [https://perma.cc/GPE7-K3C9].

[112] *Id.*

[113] 45 C.F.R. § § 160, 164(A), 164(E) (2015). The rule, in part, reads "A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter." *Id.* § 164.502(a).

[114] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182, 53182 (Aug. 14, 2002) (codified at 45 C.F.R. pts. 160, 164).

[115] *Id.*

[116] Flaherty, *supra* note 2, at 416–17.

[117] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. at 53182.

[118] *The HIPAA Privacy Rule*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/privacy/ [https://perma.cc/RKX8-ENAU].

[119] Matt Fisher, *Will the Hippo Swallow the Apple?*, HITECH ANSWERS (June 12, 2014), http://www.hitechanswers.net/apples-health-app-healthkit-hipaa/ [https://perma.cc/Q7VR-R3BA].

[120] Adam H. Greene, *When HIPAA Applies to Mobile Applications*, MOBIHEALTHNEWS (June 16 2011), http://mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications/ [https://perma.cc/5P2C-9LBS].

health app that allows individuals to follow their medication schedules or track their running distances would not fall under HIPAA because there is no involvement by a covered entity.[121] In contrast, a mobile app that health employees use in order to obtain patient healthcare information would be regulated by HIPAA because it involves a covered entity (a doctor) and protected health information.[122]

HIPAA also fails to protect consumers from the more acute problem of insurance companies receiving vast information collected from wearables. Manufacturers of wearables are not regulated by HIPAA either, so a company like Fitbit is not a HIPAA covered entity because it is not a "health care provider, health plan, employer, or health care clearinghouse."[123] However, companies like Fitbit may be regulated by HIPAA where a covered entity is involved if, for example, health employees, such as doctors, gave Fitbit direct access to patient healthcare information (or if the company voluntarily becomes HIPAA compliant).[124] In other words, generally, the HIPAA Privacy Rule does not govern information collected by companies like Fitbit because they are not a "covered entity."[125] But, HIPAA applies to insurance companies like John Hancock because insurance companies are considered a "covered entity."[126]

It seems like this HIPAA compliance solves both the problem of the underregulation of wearable devices and the more specific problem of the collection of consumer information in an insurance company scheme. But it does not.[127] The general underregulation of wearables is not solved by HIPAA because, more often than not, the companies collecting the information (i.e., technology companies or employers) will not be considered "covered entities" under the law. Moreover, even if data collection and subsequent sharing of this information constituted collection by a "covered entity" or its "business associate" (e.g., collection by John Hancock or other insurance companies) there are further restrictions to the type of data covered under this law; HIPAA protection only applies to

---

[121] *Id.*

[122] *Id.*

[123] 45 C.F.R. § 160.103 (2015); Kristen Lee, *Wearable Health Technology and HIPAA: What Is and Isn't Covered*, TECHTARGET, http://searchhealthit.techtarget.com/feature/Wearable-health-technology-and-HIPAA-What-is-and-isnt-covered [https://perma.cc/9KR9-YF5N].

[124] See *infra*, Section II.B.1.

[125] Brown, *supra* note 79, at 24–26.

[126] *See generally id.*; *see also* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 111.

[127] *See infra*, Section III.A.

"individually identifiable data."[128] This means that "[w]hen such data are aggregated for export and analysis, it arguably loses HIPAA protection because it is no longer individually identifiable."[129] Finally, the fact that HIPAA covers John Hancock's actions is not enough to prevent possible threats to privacy in this context because the threat of John Hancock's misuse of this information still exists. For example, John Hancock may use this information to take a deeper look into an individual's health profile. While a user may, on a surface level, consent to this collection of information, an individual does not necessarily consent to these hidden uses of the information. So, even if HIPAA applies to the information in questions (i.e., Fitbit data collected by a health insurance provider), HIPAA protections do not adequately protect consumers from all types of privacy threats presented.[130]

Recently, the HHS also released tools to help clarify which regulations apply to which mobile health products.[131] While these guidelines likely help companies in determining whether certain regulations apply to their product, the guidelines do not protect wearable users if there are no meaningful regulations protecting them in the first place.

2. The U.S. Food and Drug Administration

The U.S. Food and Drug Administration (FDA) is responsible for regulating mobile health apps, including app counterparts connected to wearables (e.g., the Fitbit app).[132] The Food and Drug Administration Safety and Innovation Act, signed by President Obama in 2012, gives the FDA the power to expand its authority and strengthen its ability to regulate public health.[133] The legislation therefore "allows the FDA to keep creating mobile health regulations as well as speed up the process of approving mHealth devices and apps."[134] Generally,

---

[128] *See generally id.*; *see also* U.S. DEP'T OF HEALTH & HUMAN SERVS., *supra* note 111.

[129] Brown, *supra* note 79, at 26.

[130] See *infra*, Section III.A.1.

[131] *Resources for Mobile Health App Developers*, HHS.GOV, https://www.hhs.gov/hipaa/for-professionals/special-topics/developer-portal/ [https://perma.cc/VW3A-BQVT].

[132] Vera Gruessner, *FTC's Role in Ensuring Data Security of Mobile Health Apps*, MHEALTH INTELLIGENCE (Sept. 16, 2015), http://mhealthintelligence.com/news/ftcs-role-in-ensuring-data-security-of-mobile-health-apps [https://perma.cc/F5CH-FNMY].

[133] Vera Gruessner, *Mobile Health Regulations Could Strengthen Interoperability*, MHEALTH INTELLIGENCE (Sept. 9 2015), http://mhealthintelligence.com/news/mobile-health-regulations-could-strengthen-interoperability [https://perma.cc/26G4-P6GK].

[134] *Id.*

however, FDA regulations focus on the "effectiveness and accuracy of these devices and apps rather than the privacy implications of their use."[135]

In January 2015, the FDA released "Draft Guidance For Industry and Food and Drug Administration Staff" for Low Risk Devices and released the finalized guidance on July 29, 2016.[136] Essentially, the guidance suggested that the FDA "won't vigorously regulate devices as long as they're not harmful and generally encourage healthy habits."[137] For example, the guidance stated that if a product is invasive, or "penetrates or pierces the skin or mucous membranes of the body," then the product is *not* low risk.[138] Since Fitbits do not physically penetrate the skin, they are likely considered a low-risk device and will not be rigorously regulated by the FDA. Device makers, however, are calling for the FDA to make regulations more explicit and it is unclear whether this approach will also apply to wearables.[139]

Moreover, the FDA has broad jurisdiction over medical "devices"[140] through the Food, Drug, and Cosmetic Act.[141] The act defines "device" to include instruments that are "intended for use in the diagnosis of disease or other conditions."[142] But consumer wearables likely do not fall under this category because they are not intended to treat "medical conditions";

---

[135] Brown, *supra* note 79, at 33.

[136] U.S. DEP'T OF HEALTH & HUMAN SERVS., FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES, DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2015); U.S. DEP'T OF HEALTH & HUMAN SERVS., FOOD & DRUG ADMIN., GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES, GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2016) [hereinafter FDA Guidance].

[137] Colin Lecher, *The FDA Doesn't Want to Regulate Wearables, and Device Makers Want to Keep It That Way*, VERGE (June 24, 2015), http://www.theverge.com/2015/6/24/8836049/fda-regulation-health-trackers-wearables-fitbit [https://perma.cc/VJV7-ZTZ8].

[138] FDA GUIDANCE, *supra* note 136, at 5 n.8.

[139] Lecher, *supra* note 137.

[140] Device is defined 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—(1) recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them, (2) 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 (3) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes.

21 U.S.C. § 321(h) (2012).

[141] *Id.*

[142] *Id.* § 321(h)(2).

rather, they merely promote a healthy lifestyle, thus keeping wearables out of the FDA's jurisdiction.[143]

3. The U.S. Federal Trade Commission

The Federal Trade Commission (FTC) has expressed concern in the growing use of wearables and lack of privacy laws governing the devices.[144] The FTC monitors false claims concerning mobile health apps (i.e., false claims that the device can diagnose or cure illnesses).[145] The FTC also monitors medical data breaches by non-HIPAA covered entities.[146] And while "[FTC] guidance on what constitutes reasonable cybersecurity measures isn't particularly clear or helpful, according to experts,"[147] the Commission has recently focused on bringing legal action against companies that endanger the safety of their consumers' private information.[148]

For example, since 2005, the FTC has brought numerous suits "against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers."[149] While most of these cases settled, the Third Circuit Court of Appeals recently held in favor of the FTC in an important ruling against Wyndham Worldwide Corporation.[150] The FTC sued Wyndham pursuant to 15 U.S.C. § 45(a), which prohibits "unfair or deceptive acts or practices in or affecting commerce."[151] The FTC claimed that Wyndham violated this provision because the company was hacked three times in 2008 and 2009; the hacks exposed personal and financial information of hundreds of thousand consumers and led to

---

143 Langley, *supra* note 4, at 1649–50.

144 Gruessner, *supra* note 132.

145 *Id.*; *see also* Jessica Rich, Remarks at the NAD Annual Conference 2016, at 3 (Sept. 26, 2016), https://www.ftc.gov/system/files/documents/public_statements/987463/rich_-_nad_annual_conf_2016_remarks_9-26-16.pdf [https://perma.cc/88UM-U87C].

146 Gruessner, *supra* note 132; *see also Complying with FTC's Health Breach Notification Rule*, FTC (Apr. 2010), https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule [https://perma.cc/4ZJ6-Y6FN] (discussing the Health Breach Notification Rule issued by the FTC, which applies to non-HIPAA covered entities).

147 Field, *supra* note 59.

148 *See Enforcing Privacy Promises*, FTC, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/enforcing-privacy-promises [https://perma.cc/6XZ8-GPXC].

149 FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 240 (3d Cir. 2015); *see also* Jof Enriquez, *FTC, FDA Countering Cybersecurity Risk of Wearable Devices*, MED DEVICE ONLINE (Dec. 29, 2015), https://www.meddeviceonline.com/doc/ftc-fda-countering-cybersecurity-risk-of-wearable-devices-0001 [https://perma.cc/9KHT-U8X4].

150 *See Wyndham Worldwide Corp.*, 799 F.3d at 240.

151 *Id.*; *see* 15 U.S.C. § 45(a) (2012).

$10.6 million in fraudulent charges.[152] The FTC pointed to numerous actions and omissions by Wyndham to support this claim: Wyndham allowed its hotels to "store payment card information in clear readable text," used easily guessed passwords to protect the systems, failed to use firewalls, failed to "'adequately restrict' the access of third-party vendors to its network and the servers of Wyndham-branded hotels," failed to "follow 'proper incident response procedures'" in response to hackers, and more.[153]

While the Third Circuit did not decide the case on the merits, notably, this ruling explicitly stated that 15 U.S.C. § 45(a) gives the FTC the authority to regulate cybersecurity.[154] This ruling and the recognized power that the FTC has against these unfair practices, however, only protect consumers from one part of the problem—the threat of hackers. Moreover, the FTC only has this enforcement power under the statute once there is injury to a consumer. This type of reactive measure does not adequately protect consumers from the more nuanced threats they face.

Recently, the FTC also conducted workshops and published reports that addressed threats to consumer privacy in this context. In January 2015, the FTC released a report in which it acknowledged the threats of unauthorized access to information stored in wearable devices.[155] The FTC has also suggested new protections for consumer privacy,[156] notably that app developers should provide disclosures to users and obtain consent from users when collecting "sensitive information."[157] In November 2015, the FTC conducted a workshop to examine the privacy issues surrounding cross-device tracking.[158] Cross-device tracking involves linking data streams to connect an individual's devices and gather increasing amounts of

---

[152] *Wyndham Worldwide Corp*., 799 F.3d at 240.

[153] *Id.* at 241.

[154] *Id.* at 240; *see* 15 U.S.C. § 45(a).

[155] *Internet of Things: Privacy & Security in a Connected World*, Fed. Trade Comm'n (2015) https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [https://perma.cc/E3KT-8EBD].

[156] Flaherty, *supra* note 2, at 435.

[157] FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY 23 (2013), https://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [https://perma.cc/9AT9-GHHY]; Flaherty, *supra* note 2, at 435.

[158] *See Cross-Device Tracking*, FTC, https://www.ftc.gov/news-events/events-calendar/2015/11/cross-device-tracking [https://perma.cc/6BYY-K7QK].

information from that individual.[159] FTC Chairwoman Ramirez expressed concern over the amount of data that can be collected from "cross-device" tracking.[160] At the workshop, the FTC expressed its continued efforts to protect consumers from these risks.[161] These suggestions inadequately regulate wearable privacy because they merely *suggest* ways to protect consumers rather than implement mandatory rules.

While the FTC is increasingly regulating company activity in this area, these solutions merely *react* rather than *protect* against threats because they impose liability on companies for breaches after the fact of injury. Also, these solutions fail to adequately address concerns of privacy in the insurance context, particularly how insurance companies can use data collected to assess a policyholder and possibly deny coverage or raise premiums.

4. Additional Legal Frameworks

Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA) to provide privacy protections after the fast-growing use of the internet: "The ECPA codified protections for electronic communications and extended privacy protections to e-mail and information stored by third parties."[162] Under the ECPA, it is a crime to intercept electronic communications.[163] However, the ECPA does not apply to wearables because the act does not prevent disclosure of customer records.[164] Moreover, the ECPA "explicitly exempts 'tracking devices,' which it defines as 'electronic or mechanical device[s] which permits the tracking of the movement of a person or object.'"[165]

The European Union (EU) has also expressed a growing concern for the lack of privacy regulation governing devices in the EU and worldwide.[166] The European Data Protection

---

[159] Kate Kaye, *Cross-Device Tracking Creates New Level of Privacy Concerns, FTC Says*, ADAGE (Nov. 16, 2015), http://adage.com/article/datadriven-marketing/cross-device-tracking-creates-new-privacy-concerns-ftc/301383/ [https://perma.cc/7F8Z-YFWD].

[160] *Id.*

[161] *Id.*

[162] Langley, *supra* note 4, at 1652 (citing Deirre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communication Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1558 (2004)).

[163] 18 U.S.C. § 2511 (2012).

[164] Langley, *supra* note 4, at 1652 ("Modernizing the ECPA could solve the commercial wearable problem by including sensitive health data in its statutory definition of content.").

[165] Brown, *supra* note 79, at 29–30.

[166] *See Opinion of the European Data Protection Supervisor on Mobile Health, Reconciling Technological Innovation with Data Protection*, *supra* note 25, at 2; *see also*

Supervisor (EDPS), an independent, supervising authority responsible for data protection in the EU,[167] released an opinion that expressed the following concern:

> [I]t is necessary to protect individuals' dignity and fundamental rights, particularly those of privacy and data protection. The wide use of Big Data can reduce users' control over their personal information. This is partly due to a huge unbalance between the limited information available to people and the extensive information available to entities which offer products involving the processing of this personal information.[168]

The EDPS suggested that the legislature adopt measures that require accountability in the design of these types of products, and that app designers increase transparency in relation to the use of user data.[169] It suggested that the industry promote innovation and use data collection to benefit individuals rather than harm them, and the legislature enforce stronger data security practices.[170]

The current statutory regimes are inadequate because they either do not apply to the wearable context, or they simply do not address the risks presented in situations similar to the Hancock program. While personal privacy is not left completely unregulated, different types of information are regulated under different statutory frameworks, this causes a lack of uniformity and, as shown in the case of wearables, a field of technology that is left underregulated.

III. NEW REGULATIONS ON DATA PRIVACY: PROMOTING INNOVATION AND PROTECTING PRIVACY

Striking a balance between technological advancement and protection of consumer privacy can be difficult. Consumers may overlook privacy implications in favor of fascination over new developments and technologies. Privacy may be an abstract term, but there is no doubt that most individuals expect and value a certain degree of confidentiality when sharing personal information.[171] The lack of privacy regulations governing health apps and wearables forces one to consider the

---

Frances Wheelahan et al., *Mobile Apps That Collect Health Data: Will They Be Put Under the Privacy Spotlight?*, LEXOLOGY (Sept. 8, 2015), http://www.lexology.com/library/detail.aspx?g=6f55c62e-6e9f-4a00-b16f-5536733ff672 [https://perma.cc/8VZT-86GU].

[167] *About*, EDPS, https://edps.europa.eu/about-edps [https://perma.cc/SA73-5FQT].

[168] *Opinion of the European Data Protection Supervisor on Mobile Health, Reconciling Technological Innovation with Data Protection*, *supra* note 25, at 2.

[169] *Id.*

[170] *Id.*

[171] *See generally* Katz v. United States, 389 U.S. 347, 351–52 (1967).

implications of valuing the benefits of innovation and progress over an individual's right to privacy.

The Fourth Amendment affords individuals a right to privacy.[172] In *Katz v. United States*, the Supreme Court recognized an individual's right to a reasonable expectation of privacy.[173] The court found that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[174] While it is clear from this case (and others) that the Constitution affords an individual a reasonable expectation of privacy, this concept will not apply where there are no government actors and where individuals willingly give up their privacy. Consumers consent to a certain amount of intrusion when they buy wearable devices or sign up for insurance programs that utilize these types of devices. Though, despite the lack of a Fourth Amendment violation here, it is clear that the public expects a certain amount of privacy, and it is unclear whether the public, and consumers who directly buy into this industry, are actually aware of what they are consenting to when they buy wearables and when they take part in insurance programs.

Against this uncertain backdrop, Congress must proffer an explicit solution to the ambiguity of privacy laws surrounding wearables and the new economy of wearable data information. More specifically, an applicable legal framework is necessary to deal with insurance companies offering policyholders wearable devices in exchange for discount incentives. Many solutions have been proposed in regard to privacy laws surrounding wearables in general. The trade-off of increased regulations, however, is likely "decreased liberties—both for individuals and corporations."[175] Some argue that, "personal freedoms are more important than a fleeting idea of safety."[176]

---

[172] The Fourth Amendment reads,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

[173] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[174] *Id.* at 351 (majority opinion).

[175] Alton, *supra* note 33.

[176] *Id.*

A. Alternatives That Miss the Mark

Many have argued for more explicit privacy regulations surrounding wearables.[177] Currently, the two most extreme solutions—the crux of the privacy versus innovation debate—are to either ban wearable usage altogether or leave the field underregulated, as it presently stands. The People's Liberation Army, the armed force of the People's Republic of China, has already taken the former route by "ban[ning] the use of the Apple Watch entirely."[178] This "act[] of censorship and routine banishments of Western technologies [isn't] exactly new, [but] their take-no-chances stance reflects a very real, logical concern."[179] Neither of these two options seems plausible in the United States because banning these devices completely strips individuals and businesses from participating in beneficial health initiatives, and underregulation leaves consumers vulnerable to privacy threats. Moreover, a complete ban undermines this nation's dedication "To Promote the Progress of Science and useful Arts."[180] Proper regulation is required in order for the law to reflect a preservation of a reasonable expectation of privacy while also promoting innovativeness and efficiency.

In between these two extreme positions—banning wearables altogether or leaving the area underregulated—lies a myriad of possibilities such as amending current regulations to apply to larger contexts, or relying on companies to properly protect consumer information. But many of these proposed alternatives miss the mark. None of these solutions solve both the large-scale issue of underregulation, or the more discrete issue created by schemes like the Hancock program.

1. Company Action to Ensure Customer Privacy

One way consumer data can be protected is through company action. Companies and manufacturers know consumers will not purchase their products if they do not have a reasonable privacy policy.[181] As a result, many companies are

---

[177] *See* Alton, *supra* note 33; Carl Weinschenk, *Security and Privacy Issues Surround Wearables*, IT BUS. EDGE (Aug. 24, 2014), http://www.itbusinessedge.com/blogs/data-and-telecom/security-and-privacy-issues-surround-wearables.html [https://perma.cc/WX6A-MCMU]; *see also* Gruessner, *supra* note 133 ("[M]obile health regulations will need to focus on patient data security and privacy in order to keep patients' identities safe and protected from data breaches or HIPAA violations.").

[178] Alton, *supra* note 33.

[179] *Id.*

[180] U.S. CONST. art. I, § 8.

[181] Field, *supra* note 59.

changing their policies to reflect the desire for greater consumer privacy.[182] A policy of "transparency" may protect consumers from the negative consequences of data collection: "[A]pp developers can make greater efforts to secure their apps and clearly explain their privacy policies. Device makers like Apple and Google can go on record about the potential vulnerabilities of their devices and inform the public about the best ways to protect themselves."[183]

Fitbit Inc. changed its privacy policy "to reassure users that they don't sell any identifying data."[184] On September 16, 2015, Fitbit announced that it "supports HIPAA compliance" in efforts "to more effectively integrate with HIPAA-covered entities, including corporate wellness partners, health plans and self-insured employers."[185] The privacy policy promises its users that Fitbit does not "sell data that could identify you to anyone, anywhere, anytime" and that Fitbit "only share[s data] when you tell us to, if we're required to by law or to protect Fitbit."[186]

These actions, while beneficial, fail to solve the larger problem of underregulation in the wearable context because not all wearable companies will opt into HIPAA compliance, particularly if wearable companies send the information to employers, financial institutions, or other entities that are not considered "covered entities" under HIPAA. These actions by Fitbit also fail to protect consumers from insurance companies viewing their personal information and the risk that their data may be exposed to hackers, because while Fitbit may not sell consumer data, insurance companies that are given access to a policyholder's Fitbit data—pursuant to permission given by the policyholder—will still have access and a full view of the consumer's personal information. The insurance company's full view of a patient's Fitbit information can leave the consumer open to hackers targeting the insurance company now. Moreover, consumers will have new dangers to face, such as the possibility that insurance companies will use the information gathered improperly (i.e., to deny coverage or increase their premiums).

---

[182] *Id.*

[183] Alton, *supra* note 33.

[184] Field, *supra* note 59.

[185] Press Release, Fitbit, Fitbit Extends Corporate Wellness Offering with HIPAA Compliant Offerings (Sept. 16, 2015), https://investor.fitbit.com/files/doc_news/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities.pdf [https://perma.cc/V23C-RA29].

[186] *Let's Talk About Privacy, Publically*, FITBIT (2017), http://www.fitbit.com/privacy [https://perma.cc/7RS6-6TJH] (Fitbit privacy policy).

2. Expand Existing Regulations

Another solution involves updating existing regulations to include wearable devices—a technology that was not foreseen by most of the laws regulating data protection today. For example, Congress can simply update the ECPA to include sensitive health data in its statutory definition of content and, therefore, cover wearable devices. Any amendment should also remove the exemption of "tracking devices" from the act's coverage.[187] Congress could also amend HIPAA, which, as argued above, likely already applies to insurance companies offering policyholders discounts in exchange for information.[188] This solution would *require* companies like Fitbit to comply with HIPAA regulations. Generally, this solution involves expanding the definition of "covered entities" to include "employers, app developers, and wearable device manufacturers."[189] In doing so, these entities would be forced, under the law, to meet the requirements of the Privacy Rule and other HIPAA provisions, including rules that require these entities to take certain steps to "ensure the confidentiality and integrity of electronic personal health information" and "protect[] against the use[] and disclosure of such information."[190]

The argument for the expansion of HIPAA makes sense considering the legislative history of the law. The HIPAA Privacy Rule was enacted in response to the increase in healthcare institutions' ability to transfer information electronically.[191] This increase in the avenues of transferability of PHI created a fear of misuse of that information.[192] This is precisely the issue here. At the time the Privacy Rule was enacted, it was likely hard for legislators to imagine the expansion and use of wearables in the healthcare industry today.

An expansion of HIPAA may mean expanding the definition of covered entities to encompass a wider range of entities.[193] In other words, this would expand the regulation to require more apps and devices to be HIPAA-compliant.[194] This solution would only address the broader privacy issues resulting from a lack of regulations governing wearable devices, generally.

---

187 *See* Langley, *supra* note 4, at 1642–43, 1655 n.108.

188 Field, *supra* note 59.

189 Brown, *supra* note 79, at 46.

190 *Id.* at 46–47 (citing HIPAA Privacy Rule, 45 C.F.R. pts. 160, 164(A), (E) (2003)).

191 Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53182, 53182 (Aug. 14, 2002).

192 Flaherty, *supra* note 2, at 417.

193 *Id.* at 418.

194 *Id.* at 436.

An expansion of HIPAA will not be sufficient to address the more discrete issue of personal health data being transferred to insurance companies, however, because it is not a proactive solution but rather a procedure that merely responds to privacy breaches.

There are other consequences to consider in proposing this solution. For example, an expansion of this regulation may disincentivize app developers and device makers from developing new, beneficial products because they will incur the costs of implementing these new procedures and covering any liability damages that may result.[195] Additionally, HIPAA is geared toward protecting consumers, rather than doctors or wearable device creators, and an expansion of patient protections may result in increased liability for doctors. For instance, "some have suggested that doctors who recommend certain privacy-exposing apps to their patients could be liable for violating HIPAA."[196] Also, while the initial purpose of the Privacy Rule was to respond to the increase in healthcare institutions' ability to transfer information electronically, the law was not meant to address the ability of insurance companies to make use of this information themselves (i.e., to view a full picture of their policyholders health and other information).

In regard to the more discrete issue, even if HIPAA already applies to John Hancock's actions, consumers still face the risk of data hackers and the internal uses of information transferred to insurance providers. Also, while it is not within the scope of this note, the extension of HIPAA alone fails to solve other possible uses of this type of data collected from wearables (e.g., in the employee-employer relationship).

3. Why Applying HIPAA Will Not Be Enough

Even where HIPAA applies, its application is not a complete shield to the consequences of the expanding use of wearables. According to the HHS, the HIPAA Privacy Rule:

> [R]equires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health

---

[195] *Id.*

[196] *Id.* (citing Sue Ter Maat, *Health, Fitness Apps Pose HIPAA Risks for Doctors,* AM. MED. NEWS (Aug. 5, 2013), http://www.amednews.com/article/20130805/business/130809993/7/ [https://perma.cc/5G4L-G62C]).

> information, including rights to examine and obtain a copy of their health records, and to request corrections.[197]

In other words, HIPAA requires that personal health information is protected and not shared, and provides procedures in the case of data breaches. In many ways, the HIPAA Privacy Rule does not protect the issue at hand here. As a result of the program implemented by John Hancock, life insurance companies will have access to a much larger image of a policyholder's personal health. Even if HIPAA applied in this context, the Privacy Rule would not prohibit an insurance company from viewing this full image of a policyholder's health information or from allowing insurance companies to track other information unbeknown to policyholders.

In general, life insurers require a medical checkup and are "increasingly checking hobbies, credit scores and driving records—even, in some cases, web-surfing habits—to decide who's a risk and who's not."[198] If that does not seem invasive enough, an additional eye through a device worn on your arm only increases this monitoring. The HIPAA Privacy Rule, if explicitly extended to cover this activity, would not protect consumers from the risks of handing their data over to their insurer.[199] Not only do consumers still face the threat of possible hacks or breaches, but insurance companies may still use this information to deny coverage or raise insurance premiums.

Despite the fact that HIPAA undoubtedly covers the healthcare industry, a high number of HIPAA breaches has left consumer information unprotected and subject to theft.[200] There have been 29.3 million HIPAA data breaches between 2009 and February 2014.[201] The number of these breaches increased between 2012 and February 2014 by 138%.[202] In 2013, 5447 out of 90,000 data breach complaints to the HHS went unresolved.[203] These numbers do not even tell the full story, as "[m]any healthcare breaches still go unreported" and "breaches

---

[197] *The HIPAA Privacy Rule*, *supra* note 118.

[198] Jilian Mincer, *10 Things Life Insurers Won't Tell You*, MARKET WATCH (June 30, 2011), http://www.marketwatch.com/story/10-things-life-insurers-wont-tell-you-1308333194735 [https://perma.cc/934H-5AX4].

[199] *Summary of the HIPAA Privacy Rule*, *supra* note 110.

[200] *Healthcare Security Breaches Cost $31B and Growing (Infographic)*, HIT CONSULTANT (Sept. 15, 2015), http://hitconsultant.net/2015/09/15/healthcare-security-breaches-cost-31b/ [https://perma.cc/28MP-R8UW]; *see also* Erin McCann, *HIPAA Data Breaches Climb 138 Percent*, HEALTHCARE IT NEWS (Feb. 6, 2014), http://www.healthcareitnews.com/news/hipaa-data-breaches-climb-138-percent [https://perma.cc/A4Y2-73RW].

[201] McCann, *supra* note 200.

[202] *Id.*

[203] *Id.*

involving the health records of fewer than 500 individuals are not required to be publicly reported."[204] These numbers show that while HIPAA does instill safeguards for the consumer, the regulation itself fails to adequately protect consumer privacy information—the information is nonetheless subject to breach.

It is undeniable that as the use of wearables grows, both within and outside of the healthcare field, the number of data breaches will only increase unless there is a change. Data breaches are essentially equivalent to having no privacy law at all. In the end, consumer data is released. An expansion of HIPAA's definition of "covered entities" will not necessarily protect against this threat.

IV. THE U.S. GOVERNMENT SHOULD ADOPT REGULATIONS MIRRORING THOSE OF THE GENERAL DATA PROTECTION REGULATION

A solution that completely dispenses with the option of implementing programs similar to the Hancock program goes too far by stripping individuals of their rights and hindering innovation. As long as consumers consent to this type of monitoring, it would be too limiting to forbid this type of program. In fact, this type of program has numerous benefits for a consenting, aware consumer. Even if HIPAA applies in this context, however, insurance companies should be restricted in terms of the type of data they collect and how they utilize that data. At a minimum, insurance companies should be required to tell users how they are using their information and give users the option to control its usage and existence. In the same vein, many have argued that new regulations are necessary to reflect current privacy concerns, especially in the digital age: "government organizations can step in to create some much-needed regulations about user privacy and corporate privacy policies."[205]

The first step in providing consumers with data protection in the context of the Hancock program, and similar programs, is for insurance companies to inform policyholders of exactly what data is being collected and exactly how that data is being used. The FTC Chairwoman argued that, "companies should only collect and keep information needed for a specific business purpose."[206] The EDPS suggests similar implementation

---

[204] *Id.*
[205] Alton, *supra* note 33.
[206] Ramirez, *supra* note 77, at 7.

guidelines: "[t]he EDPS recommends improvements to security requirements, 'anonymisation' techniques, greater accountability of data-collectors and improved mechanisms for obtaining consent where a person's data will be used for historical, statistical or scientific research."[207] Not only would mandatory security requirements and data anonymization techniques reduce data breaches and minimize the risk of hackers, but these rules would also ensure that insurance companies inform policyholders of exactly what data their Fitbits (or other wearable) send them and *how* they are using that data to calculate premiums. In this context, that would mean that insurance companies, like John Hancock, would be required to fully inform their policyholders. That way, consumers could either knowingly consent to the collection and usage—or not.

The United States should adopt mandatory regulations that mirror both the EDPS recommendations and the specific provisions of the General Data Protection Law (GDPR) anticipated by the European Commission. Specific provisions in a single data protection law could afford adequate protections to consumers who are unaware of how their data is being used. The law could also require stronger data encryption procedures, use of firewalls, and other mechanisms to ensure the protection of consumer data and minimize the threat of hackers and breaches. One standard of data protection law will also solve the larger problem of the lack of regulation regarding data collection from a federal level, thereby creating national uniformity for data protection and combating future privacy issues resulting from ever-increasing technological expansion.

In January 2012, the European Commission proposed a unified data protection law, the GDPR,[208] designed to strengthen privacy rights in the mobile health field.[209] Under this new regulation, which was approved on April 14, 2016,[210] principles and policy suggestions for data protections become legal obligations rather than mere recommendations.[211] Professor Rotenberg and Professor Jacobs described the regulations as "the natural evolution of the newest legal instrument to safeguard the

---

[207] Wheelahan et al., *supra* note 166.

[208] *See European Commission Proposal for a Regulation of the European Parliament and of Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, ch.I art.4, COM (2012) 11 final (Jan. 25, 2012) [hereinafter Commission Proposal].

[209] Wheelahan et al., *supra* note 166.

[210] *GDPR Portal: Site Overview*, EUGDPR, http://www.eugdpr.org/ [https://perma.cc/2QCK-ZBPY].

[211] *Id.*

modern right to privacy."[212] The European Commission hopes that this comprehensive reform of the 1995 EU Data Protection Directive will "help reinforce consumer confidence in online services, providing a much needed boost to growth, jobs and innovation in Europe."[213]

Specifically, the GDPR responds to two main problems presented by the EU Data Protection Directive of 1995. First, "the EU Data Protection Directive of 1995 did not adequately address rapidly advancing technological developments."[214] "Second, the previous EU . . . regulations created a patchwork of rules" that failed to protect individual privacy and failed to provide uniformity that is necessary for business growth.[215] An adoption of regulations that mirror those of the GDPR would allow the United States to respond to privacy issues related to an increase in technology and also promote uniformity of data protection laws throughout the country, across fields (e.g., health and telecommunications), and internationally.

In general, the GDPR protects the "personal information" of "data subjects." The proposal defines "data subjects" as "an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used" and defines "personal data" as "any information relating to a data subject."[216] The broad definitions of these terms allow the proposed regulation to provide comprehensive protection of individuals, especially since it is getting easier to identify individuals based on less information.[217] Similarly, this type of broad protection would benefit the United States because the nation faces similar privacy dangers that coincide with an increasing ability to

---

[212] Marc Rotenberg & David Jacobs, *Updating the Law of Information Privacy: The New Framework of the European Union*, *in* PRIVACY LAW AND SOCIETY 1557 (Anita L. Allen & Marc Rotenberg eds., 3d ed. 2016).

[213] European Commission, Press Release 1P/21/46, The Commission, Commission Proposes A Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses at 1 (Jan. 25, 2012).

[214] Rotenberg & Jacobs, *supra* note 212, at 1559.

[215] *Id.* The 1995 Directive was just that—a directive. Therefore, this left room for differing implementations in member states' national laws. *How Did We Get Here?*, EUGDPR, http://www.eugdpr.org/how-did-we-get-here-.html [https://perma.cc/8YXV-YK65]. The new "Regulation will establish a single, pan-European law for data protection, replacing the current inconsistent patchwork of national laws. Companies will deal with one law, not 28." European Commission Fact Sheet, Data Protection Day 2015: Concluding the EU Data Protection Reform Essential for the Digital Single Market (Jan. 28, 2015).

[216] Commission Proposal, *supra* note 208.

[217] EUR. DIGITAL RIGHTS, KEY ASPECTS OF THE PROPOSED GENERAL DATA PROTECTION REGULATION EXPLAINED: WHAT ARE THEY? WHY ARE THEY IMPORTANT? WHAT ARE COMMON MISCONCEPTIONS? WHAT CAN BE IMPROVED? 2, https://edri.org/files/GDPR-key-issues-explained.pdf [https://perma.cc/6GU7-4QWV].

identify individuals based on less information. These broad protections would clearly apply to policyholders of programs like the Hancock program where the data being collected meets this threshold, but it would also apply to other uses of wearables.[218]

"The GDPR is intended to strengthen consumer data protection rights by facilitating individual control over personal information."[219] Therefore, the GDPR requires that "the data controller must obtain written, explicit consent" to collect data on an individual.[220] Under the proposed regulation, "implicit consent" is impermissible and does not provide grounds for data processing.[221] Where a consumer gives explicit consent,[222] however, a company can process the collected data for the specified purpose. Moreover, the GDPR "grants substantive rights to data subjects" where individuals have the right to withdraw his or her consent at any time: "[t]he data subject will be able to require a data collector to erase the data subject's information if there is no legitimate reason for retaining it."[223]

The GDPR establishes that "[p]ersonal data must be[] processed lawfully, fairly and in a transparent manner in relation to the data subject."[224] This requirement codifies recommendations previously proposed by U.S. government entities[225] and "requires data collectors to implement transparent and easily accessible data processing policies, which must be written in clear, plain language."[226] This transparency provision allows individuals to understand the data protections associated with their sharing of personal information.[227]

---

218 *See supra* Section I.A.

219 Rotenberg & Jacobs, *supra* note 212, at 1559.

220 *Id.*; *see also* Commission Proposal, *supra* note 208, at 21.

221 Commission Proposal, *supra* note 208, at 43.

222 The Proposal defines "explicit consent" as:

> Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data, including by ticking a box when visiting an Internet website or by any other statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of their personal data.

Id.

223 *Id.*; Rotenberg & Jacobs, *supra* note 212, at 1559.

224 Commission Proposal for a Regulation of the European Parliament and of Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, ch.II art.5(a), COM (2012) 11 final (Jan. 25, 2012).

225 *See supra* pp. 1738–40.

226 Rotenberg & Jacobs, *supra* note 212, at 1559–60.

227 *See id.*

Also, the GDPR requires that data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes."[228] A "compatible" purpose would include, for example, processing personal data for IT security.[229] Incompatible purposes, however, would include purposes not related to the initial purpose for gathering the information, such as telecommunications data retention in which the data is initially collected for billing and further processed for law-enforcement use.[230] This type of regulation would ensure that data collection and data processing remain narrowly tailored.

The proposal also requires that "personal data" be "adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed . . . , accurate and kept up to date," and "kept in form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed."[231] Moreover, personal data can only be processed if one of the following applies: (1) the data subject consents; or the processing is necessary, (2) "for the performance of a contract" with the data subject, (3) to fulfill "a legal obligation," (3) to "protect the vital interests of the data subject," (4) for the "public interest," or (5) for "legitimate interests" except where outweighed by the interests or "fundamental rights" of the data subject.[232]

While many of the GDPR regulations mirror the EDPS recommendations, the EDPS solution will likely not remedy the risks of the Hancock program. As mentioned, the use of wearables is only expanding. However, the EDPS's recommendation does not afford individuals their deserved protection because it is a mere recommendation, not a mandatory requirement. An adoption of regulations that mirror those of the GDPR will ensure the preservation of individual privacy, allow for business growth, and promote uniformity.

If the United States adopts regulations mirroring that of the GDPR, these regulations will protect consumer privacy in the context of programs such as that implemented by John Hancock. The explicit consent requirement is the most applicable and useful in the context of the Hancock program. This type of provision would give consumers the protection necessary to maintain their reasonable expectation of privacy

---

228 Commission Proposal, *supra* note 208, at 43.
229 *Id.*
230 *Id.*
231 *Id.*
232 *Id* at 44.

because it provides them with full control of the information that data collectors receive. Moreover, the provision still affords companies the freedom to explore innovative avenues that require data collection and processing by allowing the collection and processing of data so long as consent is given. The consent requirement is moot, however, without the transparency requirement.

The "transparency principle" requires that insurance companies and Fitbit remain transparent and disclose how the collected data may be used. This requirement, combined with the consent requirement, would allow individuals to make educated decisions concerning the sharing of their personal health information.

A provision in a general data protection law scheme that requires data controllers to collect data for only a specific, compatible purpose would also protect consumer rights. If insurance companies collect information concerning policyholders' health information for the purpose of calculating and creating more specific policy costs and monitoring activities to give those policyholders discounts, then the further processing of the data for other uses would be illegal. This limitation on data collection also reduces the threat that hackers present because it minimizes the amount of information available about any one individual.

If a regulation resembling the GDPR is adopted, a problem still may exist where policyholders who opt out of the Hancock program will be at a disadvantage compared to those policyholders who choose to provide personal health information to insurance companies. Even policyholders who join the program may be at a disadvantage if they choose to withhold some of their information. Doughty explained that, "[y]ou do not have to send us any data you are not comfortable with," but the "trade-off is you won't get points for that."[233] With this type of regulation in place, policyholders can choose for themselves whether or not to provide Hancock with their personal information and thereby receive a discount on their premium. The explicit consent and transparency principle allows users to make educated decisions on these matters. If consumers choose not to explicitly consent to the data collection, they can rest assured that their data will not be processed.

A regulation resembling the GDPR gives data subjects substantive rights that would allow them to make informed decisions regarding their personal privacy. Moreover, the adoption of this type of regulation would allow the United

[233] Bernard, *supra* note 51.

States to create data protection privacy laws that establish uniformity of the law both nationally and internationally.

CONCLUSION

In today's world, the growing use of wearables presents technological advances that many have only dreamt of. But the use of these devices comes with risks. The current regulations surrounding privacy and personal health information are inadequate; they do not apply to the wearable-device context and they fail to protect consumers from the risks of data sharing and serious threats of hackers and data breaches. These risks only increase as technology improves and the uses of different technologies increase. This failure in the law requires that the government adopt new laws to regulate this industry more explicitly and stringently in order to protect privacy rights of consumers and create uniformity in the law. However, the government must also recognize the rights of individuals to create, innovate, and even use this type of technology. Insurance companies should be allowed to implement this type of program as long as there is customer consent and awareness. However, the government must restrict the type of information insurance companies are gathering and the manner in which these companies use, share, and protect this information.

Alexandra Troiano[†]

[†] J.D. Candidate, Brooklyn Law School, 2017; B.A., Queens College 2014. I would like to thank Jessica Schneider, Valentina Lumaj, and the rest of the *Brooklyn Law Review* staff for all of their time and effort not only on this note, but on this entire issue. I would also like to thank my mom, Rosann Troiano, for her encouragement and support, and my dad, Marco Troiano, for showing me the true value of hard work.