FIT TO WORK:
IMPROVING THE SECURITY OF MONITORED EMPLOYEES' HEALTH DATA

Elizabeth A. Brown[1]

INTRODUCTION

Imagine coming to work one day and finding that your employer has given everyone in the company a wearable FitBit health monitor, free of charge. You pop the FitBit on, grateful for another bit of help in managing the health concerns that nag at you persistently but which never quite rise to the top of your priority list. At your next performance review, your supervisor expresses concern about your anxiety levels. Although your work output is slightly off, she notes, there has been a correlation in your lack of sleep and exercise, and she suspects you are depressed. You wonder how your employer might know these things, whether or not they are true, and then you remember the FitBit. Your supervisor then tells you that the promotion you had wanted is going to a colleague who is "better equipped to handle the demands of the job." You interview for another job, and are asked to provide the password to the HealthDrive account that centralizes the fitness data all the apps on your iPhone collect about you during the day.

Similar scenarios are playing out now in workplaces across the country, and will do so more frequently as the personal health sensor market and employee monitoring trends continue to grow. Employers are making key decisions based on employees' biometric data, collected from specialized devices like a FitBit or the health-related apps installed on mobile phones. BP, for example, adjusts its employees' health care premiums depending on how much physical activity their wearable FitBit devices monitor – devices that BP provides to thousands of employees, their spouses, and retirees for free.[2] These programs are not always optional. Employers are already starting to require their workers to submit health metrics or pay a fine. For example, CVS Pharmacy demands that every one of the 200,000 employees who use its health plan provide certain information about their weight, glucose levels, and body fat.[3] Although CVS calls its plan "voluntary," covered workers who refuse to provide this information must pay a fine of $50 per month.

Gathering employee data from health monitoring devices and apps provides a substantial benefit to employers and poses substantial risks to employees. The benefits include a relatively user-friendly means of improving health and, correspondingly, reducing workplace losses due to illness and absence. Incidence of obesity, adult onset diabetes, and many other serious health conditions that have a behavioral component are at record levels in the United States. Health monitoring devices and apps claim great success in improving weight, BMI, and heart rate.

---

[1] Assistant Professor of Business Law, Bentley University. The author wishes to thank Sharon Patton for her invaluable assistance with this article. This is an iteration of a work that is forthcoming in the Yale Journal of Health Policy, Law and Ethics.

[2] Parmy Olson and Aaron Tilley, *The Quantified Other: Nest and Fitbit Chase a Lucrative Side Business*, FORBES.COM (April 17, 2014 4:30 a.m.), http://www.forbes.com/sites/parmyolson/2014/04/17/the-quantified-other-nest-and-fitbit-chase-a-lucrative-side-business/.

[3] Steve Osunsami, *CVS Pharmacy Wants Workers' Health Information, or They'll Pay a Fine*, ABCNEWS.GO.COM BLOG (March 20, 2013, 7:43 am), http://abcnews.go.com/blogs/health/2013/03/20/cvs-pharmacy-wants-workers-health-information-or-theyll-pay-a-fine/.

The risks, however, include the potential for adverse employment decisions, discrimination, and invasions of privacy rights that no federal law currently prohibits. The increasing coalescence of fitness-related data from apps and devices makes it increasingly likely that employers will monitor and act on employee's health data. Each data point is valuable in itself, and even more so in combination. Greater access to both heart rate data and sleep patterns, for example, might give an employer more insight into an employee's overall health than either input alone. Legal scholars have started to ask whether such monitoring is sufficiently limited by existing laws.[4] What limits employers from getting and using this data for various potentially undesirable (if not illegal) purposes?

In this article, I argue that federal law does not do enough to protect employees' health and fitness data from potential misuse, while employers have every incentive to use this data in hiring, promotion, and related decisions, and that two specific remedies would do much to curtail the improper use of employee health and fitness data.

This article proceeds in four sections. Section I describes the growth of self-monitoring apps, devices, and other sensor-enabled technology that can monitor a wide range of data related to an employee's health and fitness and the relationship of this growth to both the Quantified Self movement and the Internet of Things.[5] Section II explains the increasing use of employee monitoring through a wide range of sensors, including wearable devices, and the potential uses of that health and fitness data. Section III explores the various regulations and agency actions that might protect employees from the potential misuse of their health and fitness data and the shortcomings of each. In Section IV, I propose two specific measures that would help ameliorate the ineffective legal protections that currently exist in this context. In order to improve employee notice of and control over the disclosure of their health data, I recommend the adoption of a mandatory privacy labeling law for health-related devices and apps to be enacted and enforced by the Federal Trade Commission (FTC). As a complementary measure, I also recommend that HIPAA be amended so that its protections extend to the health-related data that employers may acquire about their employees. The article concludes with suggestions for additional scholarly discussion.

I. Employees Generate Health and Fitness Data Through Increasingly Ubiquitous Sensors.

The wearable health technology market is growing fast. Every January, technology cognoscenti descend on Las Vegas for the International Consumer Electronics Show (CES), one of the largest electronics shows in the world with over 2 million square feet of exhibition space.[6] In 2014, the Wearable and Fitness sections took up a few hundred square feet of space at CES. In 2015, the Wearable and Fitness categories together took up almost half of the cavernous exhibition hall.[7]

---

[4] *See, e.g.*, Scott R. Peppet, *Regulating the Internet of Things: First Steps Towards Managing Discrimination, Privacy, Security and Consent*, 93 TEX. L. REV. 85 (November 2014).

[5] The technology described in Section I and throughout the paper can be used by any consumer, but I use the term "employee" because the focus of this paper is on the impact of such technological advances in the employment context.

[6] *See* 2014 International CES, The Global Stage for Innovation, Attendees Audit Summary Results, *available at* https://www.cesweb.org/CES/media/2014/landing%20pages/why%20attend%20ces/2014-Audit-Summary_web.pdf.

[7] Daniel Cooper, *2015 is the year that wearables begin to grow up*, ENDGADGET.COM (January 10th 2015, 1:13 am), http://www.endgadget.com/2015/01/10/2015-ces-wearables-wrap-up/.

The mobile health market includes a range of consumer devices equipped with sensors and software-based apps that help monitor and collect health-related data. That market is expected to grow eight-fold in less than ten years, from $5.1 billion in 2013 to $41.8 billion in 2023.[8] The number of wearable fitness devices sold annually is expected nearly to triple between 2014 and 2018.[9]

One of the most popular examples is the FitBit. FitBit makes several versions of a wearable device that "tracks every part of your day—including activity, exercise, food, weight and sleep," according to its website[10]. Specifically, FitBit devices record "sleep tracking," "auto sleep detection," continuous heart rate, floors climbed, and "active minutes," although the specific combination of surveillance features depends on the model. [11] Some models also track your GPS location, and can synchronize and send information wirelessly as well.[12]

FitBit makes just a few of the thousands of health-monitoring devices and mobile phone apps that record personal health data. These devices are so popular that one in ten Americans over the age of 18 now owns an activity tracker. [13]

Wearables can measure many other kinds of data that employers would value, such as wellbeing and mood. Zensorium's being, introduced at CES in 2015, is a watch-like device that indicates whether the wearer's mood is Distress, Excited, Normal or Calm.[14] Other wearable technology promises to influence mood directly. Thync, a company founded by Harvard neuroscientists, developed a sensor that attaches to the temple and changes the wearer's mental state either to energized or sleepy.[15]

Apps that help measure aspects of health and fitness are growing exponentially as well. According to Google, the "health and fitness" category was the fastest growing app industry segment in 2014.[16] Industry analysts estimate that there are now 100,000 mobile health apps available for Android and iOS, twice as many as there were in 2012.[17] The global health and fitness mobile app market, now worth about $4 billion, is expected to more than quadruple to $26 billion by 2017.[18] The FDA estimates that 500 million smartphone users now use or will soon use at least one health care app.[19]

---

[8] Carole Jacques, *Mobile Health Devices Market to grow 8-Fold to $41.8 Billion in 2023*, LUXRESEARCHINC.COM, http://www.luxresearchinc.com/news-and-events/press-releases/read/mobile-health-devices-market-grow-8-fold-418-billion-2023.

[9] Fred Pennic, *Fitness Devices to Dominate the Wearables Market Until 2018*, HITCONSULTANT.NET (November 25, 2014), http://hitconsultant.net/2014/11/25/fitness-devices-to-dominate-the-wearables-market-until-2018/.

[10] FITBIT, https://www.fitbit.com/whyfitbit, last visited July 16, 2015.

[11] FITBIT, https://www.fitbit.com/compare last visited July 16, 2015.

[12] *Id.*

[13] Dan Ledger and Daniel McCaffrey, *Inside Wearables: How the Science of Human Behavior Change Offers the Secret to Long-Term Engagement*, ENDEAVOR PARTNERS, (JANUARY 2014), *available at* http://endeavourpartners.net/assets/Wearables-and-the-Science-of-Human-Behavior-Change-EP4.pdf, at 2. For an overview of the various types of consumer sensor devices, *see* Peppet, *supra* note 4, at 98-116.

[14] Nicole Lee, *Zensorium's 'Being' is a fitness wearable that promises to track your mood as well*, ENDGADGET.COM (January 4, 2015, 9:40 pm), http://www.engadget.com/2015/01/04/zensorium-being/.

[15] Kevin Bullis, *Device Changes Your Mood With A Zap To The Head*, TECHNOLOGYREVIEW.COM (November 10, 2014), http://www.technologyreview.com/news/532321/device-changes-your-mood-with-a-zap-to-the-head/.

[16] Andy Boxhall, *2014 is the Year of Health and Fitness Apps, Says Google*, DIGITALTRENDS.COM (December 11, 2014), http://www.digitaltrends.com/mobile/google-play-store-2014-most-downloaded-apps/.

[17] *Id.*

[18] *Id.*

[19] FDA News Release, *FDA Outlines Oversight of Mobile Medical Applications*, FDA.GOV ((July 19, 2011), http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm263340.htm.

A. Health and Fitness Data Collection Is On the Upswing.

Never have employers had so much new and valuable data about their workforce released to them within such a short time. The rapidly increasing collection of health-related data from wearable devices and apps sits at the convergence of three trends: (1) the Internet of Things, (2) the Quantified Self Movement and (3) the rise of the health data platform.

1. The Internet of Things

The Internet of Things is the shorthand term given to the increasing interconnectivity of common objects.[20] Examples include refrigerators that detect when you are low on milk and populate grocery lists which pop up on your cell phone and beds that self-adjust to cool you down or heat you up, as needed, and remotely start your coffee maker within a certain time after you get up. The number of things connected to the Internet surpassed the number of people connected to the Internet in 2009.[21] By the end of 2015, some experts estimate that there will be 25 billion connected devices and that that number will double by 2020.[22] Three and a half billion sensors are in commerce now, and some predict that there will be trillions of sensors within ten years.[23]

These health-monitoring sensors are part of a global trend toward more ubiquitous forms of monitoring. For example, parts of cities are now being fitted with monitors, with New York and Chicago leading the way. At NYU's Center for Urban Science and Progress, a team is using ultrasensitive light sensors to determine the time households go to bed, what type of light bulbs they use, and what pollutants their buildings emit, among other data.[24] The University of Chicago has announced plans to install dozens of sensor packs on street lamps across Chicago to collect data on environmental conditions such as sound volume, wind levels, carbon-dioxide levels, and pedestrian traffic flow. "It's like a Fitbit for the city," one administrator told the Wall Street Journal.[25]

While investors, developers and manufacturers scramble to produce more interconnected devices, there is a gap between the institutional embrace of the Internet of Things and public comfort levels. In a January 2015 survey by a Nielsen company, 53 percent of respondents said they were concerned that their data might be shared without their knowledge or approval. Almost as many worried about the risk of security breaches. Of the 4,000 survey respondents, 51 percent said they were concerned that their data could be hacked by other users.[26] Whether their personal data is shared intentionally or unintentionally, these numbers suggest that just over

---

[20] Janna Anderson and Lee Rainie, *The Internet of Things Will Thrive By 2025* (May 14, 2014), www.pewinternet.org/2014/05/14/internet-of-things/.
[21] Dave Evans, Cisco Internet Bus. Solutions Grp., *The Internet of Things: How the Next Evolution of the Internet is Changing Everything* 3(2011), www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
[22] *Id.*
[23] Stanford Univ., *TSensors Summit for Trillion Sensor Roadmap*, TSENSORSSUMMIT.ORG (Oct. 23-25 2013), http://tsensorssummit.org/Resources/why%20TSensors%20Roadmap.pdf.
[24] Elizabeth Dwoskin, *They're Tracking When You Turn Off The Lights*, WSJ.COM (October 20, 2014, 9:20 pm), http://online.wsj.com/articles/theyre-tracking-when-you-turn-off-the-lights-1413854422.
[25] *Id.*
[26] Kim Gaskins, *What's holding back the Internet of things?*, VENTUREBEAT.COM (January 18, 2015, 6:58 am), http://venturebeat.com/2015/01/18/whats-holding-back-the-internet-of-things/.

half of consumers are concerned about the loss of privacy that more interconnectedness may bring. These reservations suggest that concern about potential losses of privacy have not yet outweighed the perceived benefit of the Internet of Things.

2. The Quantified Self Movement

The Quantified Self movement refers to the increasing popular demand for devices that monitor and measure an enormous range of physical data about oneself, including heart rate, weight, blood sugar, sleep patterns, and diet.

The collection of health data has already moved well beyond wearable devices. Shirts embedded with sensors are already sold by companies like OMsignal, Hexoskin and Cambridge Consultants.[27] While initially marketed to consumers who want their workout wear to measure how many reps they complete at the gym as well as their heart rate, employers can adopt similar sensor-embedded shirts as uniforms.

As early as 2011, John Rogers introduced a wearable, ultra-thin circuit that can be attached to the wearer's skin like a temporary tattoo.[28] The Epidermal Electronic System, as it is called, is capable of measuring brain, heart and muscle activity much like a traditional EEG and can transmit the data wirelessly. While initially envisioned as a medical device, the transmission of data could go to a nonmedical recipient as easily as to a doctor or a hospital. Temporary tattoos are being used to monitor and transmit other kinds of health data as well. They can monitor blood sugar levels, detecting spikes in glucose without the need for skin pricks.[29] Developers announced plans to equip future versions of these tattoos with "Bluetooth capabilities that can directly send data from the sticker to a cloud-based storage app."

The more intimate placement of health data collectors is taking more permanent forms as well. Another kind of sensor would go even farther under the skin, to coat the internal organs. Gel-based sensors that convey electrical information and other health-related data directly from the heart, lungs and kidneys are currently being tested in Japanese laboratories.[30] In Switzerland, a team of researchers has developed a blood-testing sensor that is implanted under the skin and can convey a range of health data over Bluetooth, including cholesterol levels and blood sugar levels.[31]

As sensors migrate internally, it may also become harder to turn these sensors off or remove them, making it more difficult for employees to control the flow of health-related data to the outside world. Because these kinds of devices are harder to alter, they are potentially more valuable to employers and less susceptible to employee error.

---

[27] Daniel Cooper, *Hexoskin's smart shirt feels nice, but can't tell a step from a curl,* ENDGADGET.COM (December 2, 2014 12:00 pm), http://www.engadget.com/2014/12/02/hexoskin-hands-on/; *see also* Daniel Cooper, *Your next smart shirt will make you look like an extra from 'Tron,'* ENDGADGET.COM (January 6, 2015, 4:56p.m.), http://www.engadget.com/2015/01/06/cambridge-consultants-xelflex/.

[28] Daniel Cooper, *EES packs circuits into temporary tattoos, makes medical diagnostics fashionable,* ENDGADGET.COM (August 12, 2011, 11:52 p.m.), http://www.engadget.com/2011/08/12/ees-packs-circuits-into-temporary-tattoos-makes-medical-diagnos/.

[29] Gabriella Garcia, *Temporary Tattoo-Based Glucose Monitoring*, COOLHUNTING.COM (January 26, 2015), http://www.coolhunting.com/tech/temporary-tattoo-glucose-monitoring.

[30] Jon Fingas, *Sticky sensors will monitor your body's organs,* ENDGADGET.COM (December 30, 2014, 2:18 a.m.), http://www.engadget.com/2014/12/30/sticky-organ-sensors/?ncid=txtlnkusaolp00000595.

[31] Mat Smith, *Wireless 'under the skin' prototype implant beams instant blood test read-outs to your smartphone,* ENDGADGET.COM (March 20, 2013, 7:54 a.m.), http://www.engadget.com/2013/03/20/wireless-under-the-skin-implant-can-beam-instant-blood-test-re/.

3. The Emergence of Health Data Platforms

A third relevant trend is the centralization of fitness data collected from disparate sources through dedicated software platforms. The world's largest electronics manufacturers expect interest in health and fitness monitoring to continue its explosive growth, and are making it easier for users to monitor themselves. Apple's Health app allows users to see all of their health and fitness data at a glance. As one observer put it, "you could use devices and apps from different companies -- say a Nike FuelBand, a Withings Blood Pressure Monitor and an iHealth Wireless Smart Gluco-Monitoring System -- and have information from all of them gathered in the Apple Health app, which serves as a dashboard for your health and fitness data."[32] Apple's competitor Samsung is also investing heavily in the symbiosis of disparate health and fitness monitors. In 2014, it announced the development of Samsung Architecture for Multimodal Interactions (SAMI), which centralizes data from various health-related apps and devices and makes it accessible to others, perhaps including employer-sponsored collectors.[33]

Apple and Samsung have also introduced devices that complement the health data collection features of this software. Apple's flagship devices, currently the iPhone 6 and iPhone 6 Plus, feature an M8 motion co-processor chip that improves the phones' function as a fitness monitor. The M8 allows the phones to detect what kind of physical activity the user is engaged in (e.g., running, biking or walking), estimate the distance traveled, and even the altitude thanks to a built-in barometer.[34] Samsung has introduced the Simband, an open-hardware sensor that can collect a wide range of health and fitness data in conjunction with SAMI.[35] According to Samsung, "The combination of Simband-designed sensor technology and algorithms and SAMI-based software will take individual understanding of the body to a new level—for the first time giving voice to a deeper understanding of personal health and wellness." [36] In early 2014, Samsung also unveiled the first mobile phone with an integrated heart rate monitor, its Galaxy 5.[37] The fact that Samsung and Apple both build fitness sensors into their flagship phones is a powerful indicator that more health data will be collected and potentially used by employers over time.

---

[32] Nicole Lee, *Apple: Putting doctors, trainers and nutritionists in your pocket*, ENDGADGET.COM (June 3, 2014, 9:17 p.m.), http://www.engadget.com/2014/06/03/apple-healthkit-fitness/.

[33] *See* SAMSUNG SAMI, http://developer.samsungsami.io/ (last visited July 16, 2015).

[34] Ashley Feinberg, *The iPhone 6's New M8 Chip Makes It A Truly Badass Fitness Tracker*, GIZMODO.COM (September 9, 2014, 1:32pm), http://gizmodo.com/the-iphones-new-m8-chip-makes-it-a-truly-badass-fitness-1632519058.

[35] Nicole Lee, *Samsung launches a flexible platform of sensors for wearables*, ENDGADGET.COM (May 28, 2014, 2:16pm), http://www.engadget.com/2014/05/28/samsung-launches-a-flexible-platform-of-sensors-for-wearables. Interestingly, SAMI was developed in part by Luc Julia, a former Apple engineer. *See* Samuel Gibbs, *Samsung's SAMI project is led by former Siri engineer from Apple*, THEGUARDIAN.COM (November 11, 2013, 10:12am), http://www.theguardian.com/technology/2013/nov/11/samsungs-sami-project-siri-engineer-apple.

[36] Michelle Maisto, *Apple, Samsung Taking Different Roads to Consumer Health Empowerment*, EWEEK.COM (June 9, 2014), www.eweek.com/mobile/apple-samsung-taking-different-roads-to-consumer-health-empowerment.html#sthash.6vkTyOD0.dpuf.

[37] Michelle Maisto, *Samsung Unveils Galaxy S5, Gear Fit, Galaxy Gear 2, Gear 2 Neo at MWC*, EWEEK.COM (February 25, 2014), http://www.eweek.com/mobile/slideshows/samsung-unveils-galaxy-s5-gear-fit-galaxy-gear-2-gear-2-neo-at-mwc.html.

II. Employers Have Unprecedented Access to Employees' Health and Fitness Data

Employers have every incentive to collect as much data as they may, especially when doing so increases profitability. Minimizing health insurance costs is only one example of how employee data can improve the bottom line. Using health data to inform hiring and promotion decisions is another. To what extent these uses of employee data are legal is an increasingly important question in employment and privacy law.

The explosive growth of wearable device ownership makes it easier than ever for employers to collect health and fitness data about their employees. The people most likely to use those devices are those who employers are most interested in evaluating. The rates of health tracker ownership coincide nicely with the statistical likelihood of workplace influence. The group that is most likely to own a fitness tracker is also the group most likely to be advancing at work into junior management positions, while the group that is least likely to have these devices is most likely to be retiring from the workplace altogether. People in their late 20s and early 30s have the highest rates of ownership, with 25% of survey respondents between ages 25-34 reporting that they have an activity tracker.[38] Conversely, the lowest rates of ownership are, as one might expect, among those over 65, with only 7% of that group owning such a device.[39] In a sense, the age cohort with the most to lose from employer misuse of health and fitness data is the one that is most vulnerable to that misuse.

A. New Technology Facilitates Employee Health Data Collection.

Employers are starting to collect a wide range of data from more ubiquitous and often mandatory wearable devices. The collection of health and fitness data is part of a larger trend toward electronic monitoring of individual employees. Hitachi, for example, now offers employers the Business Microscope, a kind of advanced employee security badge embedded with infrared sensors, a microphone sensor and a wireless communication device. When two employees wear these badges within a certain distance of each other, the badges recognize each other, record face time, body and behavioral data and send them to a server.[40] The badges send management data about who talks to whom, how often, where and with how much energy. It also tells employers how much time each employee spends out of their seats.

In reporting on these new devices, one journalist noted that "while privacy concerns are an obvious issue," the system "has already been shown to improve productivity. " One retail seller reported a 15% increase in average sales per customer after using the badges for ten days.[41] A similar employee monitoring badge developed by Sociometric Solutions includes a microphone that assesses the tone of voice the employee uses as well as an infrared beam that determines the speaker's position relative to other badge-wearing employees.[42] The British

---

[38] Ledger and McCaffrey, *supra* note 13, at 3.
[39] *Id.*
[40] Victoria Young, *Wearable Device Monitors Employee Productivity*, PSFK.COM, (February 10, 2014), http://www.psfk.com/2014/02/wearable-employee-productivity-tracker.html.
[41] *Id.*
[42] Vivian Giang, *Companies Are Putting Sensors on Employees To Track Their Every Move*, BUSINESSINSIDER.COM (March 14, 2013, 6:23 p.m.), http://www.businessinsider.com/tracking-employees-with-productivity-sensors-2013-3.

grocery chain Tesco uses an armband containing a Motorola device to monitor its employees' productivity and to track when they take breaks.[43]

Employers are taking advantage of the increasing availability of health and fitness data generated by interconnected apps and devices as well. For example, BP offers a program by which employees can cut $1200 from their annual insurance bills in exchange for wearing a Fitbit and logging a sufficient amount of physical activity.[44] Like other employers, BP faces rising health care costs and is looking for ways to reduce them. Providing incentives for employees to improve their health could benefit the employers as well. One Bay Area employer negotiated a $300,000 discount on its $5 million insurance costs by agreeing to share employee health data with its insurer and showing that the staff's health was improving. [45] Forty percent of their employees upload their fitness data via their Fitbit devices.[46]

Employers like BP, Cigna and Autodesk offer their employees the FitBits for free or at substantially reduced rates in a program that they can describe as a "win-win" for both sides.[47] The employers have a vested interest in their employees' health, and the employees get a significant discount on a popular device. One effect of employer-monitored wearables may be increased or longer use of the device.[48] As Jiff notes on its blog, "by encouraging employees to use their personal fitness devices in the right way, companies can motivate employees to continue using their wearables, and achieve lasting health benefits."[49]

Insurers are working closely with employers to facilitate programs like these. United Health Group, Humana, Cigna and Highmark have all developed programs that help their employer clients integrate wearable devices like the FitBit into the workplace.[50] This tech-assisted approach to employee wellness fits into a general trend of increased spending on health programs at work. According to one study, spending on corporate wellness incentives more than doubled between 2009 and 2014, with corporations now spending an average of $594 per employee annually on such programs.[51] By 2018, analysts predict that a third of fitness-tracking device sales will come from corporate wellness programs.[52]

---

[43] Claire Suddath, *Tesco Monitors Employees With Motorola Armbands***,** BLOOMBERG.COM (February 13, 2013), http://www.bloomberg.com/bw/articles/2013-02-13/tesco-monitors-employees-with-motorola-arm-bands.

[44] Adam Satariano, *Wear This Device So the Boss Knows You're Losing Weight*, BLOOMBERG.COM (Aug. 21, 2014, 1:26 p.m.), http://www.bloomberg.com/news/articles/2014-08-21/wear-this-device-so-the-boss-knows-you-re-losing-weight.

[45] *Id.*

[46] *Id.*

[47] *See* David Nield, *EMPLOYEE WELLNESS PROGRAMS NOW ONE OF FITBITS FASTEST GROWING AREAS*, DIGITALTRENDS.COM (April 19, 2014), http://www.digitaltrends.com/mobile/employee-wellness-programs-now-one-fitbits-fastest-growing-areas/.

[48] *See* Ledger and McCaffrey, *supra*, note 13.

[49] Panpan Wang, *Employers Key To Helping Consumers Take Advantage of Wearables Trend*, JIFF.SQUARESPACE.COM (September 16, 2014), http://www.jiff.squarespace.com/blog/employers-key-to-helping-consumers-take-advantage-of-wearables-trend.

[50] *Id.*

[51] *Health Care Survey Finds Spending On Corporate Wellness Incentives to Increase 15 Percent in 2014*, FIDELITY.COM (February 20, 2014), http://www.fidelity.com/inside-fidelity/employer-services/health-care-survey-finds-spending.

[52] Adrian Kingsley-Hughes, *Wearables and Health Insurance: A health bar over everyone's head*, (August 26, 2014,10:25 gmt), http://www.zdnet/article/wearables-and-health-insurance--a-health-bar-over-everyone-s-head.

B. Providers and Platforms Help Aggregate Employee Health Data.

In coming years, the amount of health-related information that can transfer from an employee to a wearable sensor will increase. Medical professionals champion the use of health data sensors, in part to improve the quality of medical treatment as doctors spend less time with patients than they have in the past.[53] Many predict that implantable or wearable sensors will send biometric data to a smartphone, continually supplementing a database of information that can help monitor health conditions. [54]

The growing demand for health and fitness data will be driven as much by employers as by the medical profession. Device manufacturers and app developers recognize the importance of employers as a revenue stream. Fitbit began selling data in bulk to employers in 2010, along with software that facilitates the translation of that data.[55] In 2014, its CEO announced that its sales to employers are one of its "one of the fastest-growing parts of Fitbit's business."[56]

Employers don't have to go through device manufacturers like FitBit, however, to collect health-related information about their employees. Startups including Pact, WelBe and Jiff also sell software that allows employers to track and collect this kind of data from any wearable device.[57] WelBe's website, for example, suggests that its software can monitor how much employees sleep, eat, drink, exercise, climb stairs, use electricity and possibly laugh.[58] It coordinates input from sources including FitBit, Garmin, MyFitnessPal, RunKeeper and Jawbone.[59] WelBe offers what it ominously calls "wellbeing coordinators" – which presumably used to be human resources managers – the ability to "create aggregated biometric reports on the fly and take a deep dive into data on employees' activity levels, financial fitness, challenge activities, and nutritional health."[60] Data aggregators such as TicTrak and Foxing also collect information from various fitness trackers.[61]

App developers find it increasingly easy and rewarding to generate data that can be centralized and transferred in this way. For example, Apple's introduction of HealthKit, in June 2014, simplified the aggregation and transfer of health related data. HealthKit is a tool that helps developers create apps that draw on a user's centralized health and fitness data, effectively allowing them to share data with and import data from other HealthKit-enabled apps.[62]

---

[53] Anick Jesdanun, *Doctors say fitness trackers, health apps can boost care*, PHYS.ORG (February 20, 2015 1:30pm), http://phys.org/news/2015-02-doctors-trackers-health-apps-boost.html.

[54] *See* ERIC TOPOL,M.D., THE CREATIVE DESTRUCTION OF MEDICINE 162-63 (2012) (describing hypothetical nano-sensor monitoring of patients' blood to detect markers of heart disease or cancers for those at high risk of such diseases).

[55] Parmy Olson, *Jawbone Jumps Into Employee Monitoring*, FORBES. COM (December 11, 2014, 7:48 a.m.), http://www.forbes.com/sites/parmyolson/2014/12/11/jawbone-employee-fitness-monitoring/.

[56] *See* Nield, *supra* note 47.

[57] *See* Olson, *supra* note 55.

[58] WELBE, https://www.welbe.com/ On this site, an embedded video without narration entitled "How Do You Live Welbe?" shows a young woman whose every move, from the moment she wakes up in the morning, appears to be recorded. It is not clear exactly how each of these data points is being recorded, as we see her with a wearable device, entering information into an app on her phone.

[59] Tom Rath, *a new version of eat, move, sleep and the welbe app*, BLOG OCTANNER.COM (January 19, 2015), http://blog.octanner.com/editor-picks/a-new-version-of-eat-move-sleep-and-the-welbe-app

[60] *See* WELBE, *supra* note 58.

[61] *See* Ledger and McCaffrey, *supra* note 13, at 4.

[62] THE HEALTHKIT FRAMEWORK, https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/

While the most direct means of data collection at work is to use employer-provided devices and apps, employers could also collect data generated by employees' own devices. Employers have already shown a willingness to use employees' personal technology to their advantage, blurring the line between personal data and workplace device. The "Bring Your Own Device" (BYOD) movement has gained ground quickly.[63] When employers give their employees electronic devices for work purposes, the employers have greater legal access to the data on those devices than anyone else. The Supreme Court has made it clear that employees using employer-provided devices have little reasonable expectation of privacy in doing so.[64] At the same time, the use of personal devices at work can give rise to serious concerns about employee privacy, intellectual property protection, and workplace discrimination. For example, at least one scholar has wondered whether the increasing use of Google Glass by employees raises the likelihood of workplace espionage and trade secret theft.[65]

C. Using Employee Health Data to Inform Employment Decisions Creates Potential Legal and Ethical Hazards.

There is ample potential for employer misuse of current and potential employees' health and fitness data. This data could inform employment decisions in nearly unlimited ways. As Professor Peppet points out, smartphone sensors can provide data from which employers can infer "a user's mood, stress levels, personality type, bipolar disorder, demographics (e.g., gender, marital status, job status, age); smoking habits, overall well-being, progression of Parkinson's disease, sleep patterns, happiness, levels of exercise, and types pf physical activity or movement." [66] It is easy to imagine a scenario where an employer, having to decide which of two candidates to promote, reviews each candidate's sleep patterns, physical activity, calorie intake and/or mood – all of which can be monitored and measured remotely – and decides based at least in part on that data.

When employers use the health and fitness data they collect to make employment decisions, including hiring and promotion, there is cause for concern.[67] As discussed further in the next section, the legal frameworks we rely on to prohibit discrimination are of little use here. Evaluating an employee for a promotion based on the employer's assessment of the likelihood that the employee will develop an unspecified health condition later in life, for example, based on the candidate's monitored physical activity levels, would not invoke disability law because no specific disability is invoked or perceived.[68] Similarly, making employment choices based even in part on sleep patterns, nutritional intake, or smoking – all of which can be measured by mobile sensors – may look like discrimination to a non-lawyer. Federal anti-discrimination laws, however, cannot protect employees against decisions made on the basis of something other than, and not necessarily correlated with, a protected class.[69]

There are other risks as well. Employers who collect health and fitness data are susceptible to security breaches, possibly leading to the unauthorized distribution of that data.

---

[63] Anisha Mehta, *"Bring Your Own Glass": The Privacy Implications of Google Glass In the Workplace*, 30 J. INFO. TECH. & PRIVACY L. 607 (2014).
[64] City of Ontario, Cal. v. Quon, 560 U.S. 746, 747 (2010).
[65] *See* Mehta, *supra* note 63.
[66] Peppet, *supra* note 4, at 115-116 (footnotes omitted).
[67] *Id.* at 118.
[68] *Id.* at 125-126.
[69] *Id.*

Such security breaches are on the rise. According to one survey, there were over 300,000 reported cases of medical identity theft in 2013, a 19% increase over the previous year. [70]

There is also the danger that in-house staff may manipulate the data collected for a variety of reasons. Employees are unlikely to check the accuracy of the health-related data their employers collect. Most people do not verify the accuracy of their health records at all. In a 2013 survey, 56 percent of respondents admitted that they do not check their medical records to determine if the health information is accurate at all.[71]

III. Federal Law Does Too Little To Protect Employee Health Data.

While several federal laws appear to prohibit employers' potential misuse of health and fitness data, as described below, significant gaps remain in the federal protection of this data. Many federal agencies and laws might address this growing problem, but none does so effectively. While states have a variety of data privacy laws, this article focuses instead on the shortcomings of the federal law that could protect employees in every state.

A. Employees May Have No Reasonable Expectation of Privacy in Sensor-Generated Health Data

An important preliminary question is whether there is any right of privacy in health-related information beyond specific regulatory protections. Whether there is a reasonable expectation of privacy under the Fourth Amendment depends on both subjective and objective standards. According to the Supreme Court in *Katz v. United States*, a person's reasonable expectation of privacy in a given context depends upon the results of a two-prong test.[72] First, a person must display an actual, subjective expectation of privacy. Second, the expectation must be one that society recognizes as reasonable.

Some have observed that consumers have ever-decreasing expectations of privacy.[73] The increasing use of personal devices at work is further eroding these expectations of privacy. [74] For that reason, under the second prong of *Katz*, it may be difficult to prove that society recognizes privacy in employee health data as reasonable. Recent studies show, however, that many people still fear losing privacy, especially as technology becomes more communicative. In a 2015 survey, privacy and security were respondents' top concerns about the Internet of Things. More than half expressed concern that their data might be shared without their knowledge or approval.[75] In addition, public expectations of health data privacy associated with HIPAA may weigh in favor of finding that society recognizes a privacy right in such data beyond the specific protections HIPAA offers.

Courts have yet to issue a detailed ruling as to whether there is a reasonable expectation of privacy in the health and fitness data employers collect from their employees. In the absence

---

[70] Ponemon Institute Research Report, *2013 Survey on Medical Identity Theft* (September 2013), *available at* https://clearwatercompliance.com/wp-content/uploads/2013/10/2013-Medical-Identity-Theft-Report-FINAL.pdf at 2

[71] *Id.* at 13.

[72] 389 U.S. 347, 361 (1967).

[73] See, e.g., Kate Murphy, *We Want Privacy, but Can't Stop Sharing*, NYTIMES.COM (October 4, 2014), http://www.nytimes.com/2014/10/05/sunday-review/we-want-privacy-but-cant-stop-sharing.html.

[74] Stephen Wu, *Employee Privacy in the Dawn of the Mobile Revolution; The Prevalence of BYODs in the Workplace Signals a Need for Companies to Revise Their Monitoring Policies*, THE RECORDER, Feb. 22, 2013.

[75] *See supra*, note 23.

of such precedent, the protections afforded by specific federal regulation, or lack thereof, become even more important.

B. Federal Regulation of Health and Fitness Data Collection is Fragmented and Insufficient.

Americans have a general sense that their personal health information should be secure. Doctors' offices regularly present us with HIPAA notices that provide a sense of reassurance about the privacy of our health records. HIPAA does not adequately protect the kind of health and fitness data generated by popular health and fitness devices and apps, however, because its scope is limited to records generated by medical professionals. Nor do any of several other federal laws that might at first appear to protect this data, as discussed in more detail below. These gaps in regulatory coverage deserve greater scholarly and public attention.

1. Health Insurance Portability and Accountability Act

The Federal Health Insurance Portability and Accountability Act of 1996, or HIPAA, was designed to protect the confidentiality of patients' health information. HIPAA, however, does not protect the kind of health and fitness data that wearable technology or fitness apps might collect.[76] When a FitBit or iPhone app tells an employer how much an employee has exercised, what her heart rate is, or how high her blood sugar levels are, that data does not fall within the scope of HIPAA protection.

According to the U.S. Department of Health and Human Services, HIPAA "provides federal protections for individually identifiable health information held by covered entities and their business associates and gives patients an array of rights with respect to that information."[77] The "covered entities" include health care providers, health plans (including insurers and HMOs) and health care "clearinghouses" that translate health information from one format to another.[78] Certain HIPAA laws also apply to the "business associates" that covered entities hire to help them carry out health care functions. HIPAA only restricts what covered entities and their business associates can do. Other entities and individuals are not so restricted.

Additionally, the information that HIPAA protects is limited to "[i]ndividually identifiable health information," which is generally limited to medical and billing records. [79] As Professor Hall has observed, the "disclosure of individually identifiable biometric data by the company that manufactures the device, sells the app, or runs the website aggregating the data does not violate HIPAA's Privacy Rule as it currently stands."[80]

2. The Americans with Disabilities Amendments Act

The Americans with Disabilities Amendment Act (ADAAA) protects against employment discrimination on the basis of an actual or perceived disability. Many kinds of

---

[76] *See* Timothy S. Hall, *The Quantified Self Movement: Legal Challenges and Benefits of Personal Biometric Data Tracking*, 7 AKRON INTELL. PROP. J. 27, 29-30.
[77] U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, UNDERSTANDING HEALTH INFORMATION PRIVACY, *available at*, http://www.hhs.gov/ocr/privacy/hipaa/understanding/.
[78] 45 C.F.R §160.103 (2014).
[79] 45 C.F.R. §§ 160.102-103 (2014).
[80] *See* Hall, *supra* note 76, at 30.

fitness data that sensors generate and employers collect, however, neither constitutes nor correlates with a disability as defined under the ADAAA.[81]

The ADAAA might limit employers' data collection practices in other ways, however. As noted earlier, the drugstore chain CVS requires its employees to submit to personal health data collection or to pay a fine. Is this kind of disclose-or-pay requirement legal? Current case law suggests that it is. One legal barrier might be the ADAAA's provision that employers cannot make "disability-related" inquiries or require prospective or current employees to undergo medical examinations unless they are job-related or subject to a business necessity exception. An inquiry is "disability-related" if an individual's response to the inquiry could reasonably be expected to disclose the presence of a protected disability. Once employment begins, the employer can make disability-related inquiries or require employees to submit to medical examinations only if they are "job-related and consistent with business necessity."

The ADAAA provides a safe harbor for employers' medical testing requirements in three situations, generally in connection with health insurance plans. Employers may make disability-related inquiries or require employees to submit to medical examinations in the following situations:

(1) an insurer, hospital or medical service company, health maintenance organization, or any agent, or entity that administers benefit plans, or similar organizations from underwriting risks, classifying risks, or administering such risks that are based on or not inconsistent with State law; or

(2) a person or organization covered by this chapter from establishing, sponsoring, observing or administering the terms of a bona fide benefit plan that are based on underwriting risks, classifying risks, or administering such risks that are based on or not inconsistent with State law; or

(3) a person or organization covered by this chapter from establishing, sponsoring, observing or administering the terms of a bona fide benefit plan that is not subject to State laws that regulate insurance. [82]

None of these safe harbor provisions may be used as a subterfuge to avoid the underlying anti-discriminatory purposes of the ADAAA. [83]

At least one court has ruled that employers may subject employees to a penalty for failing to submit to health screenings without violating the ADAAA. In 2012, the Eleventh Circuit Court of Appeals decided that Florida's Broward County did not run afoul of the ADAAA when it deducted $20.00 from each bi-weekly paycheck of employees who refused to submit to a wellness program.[84] The County's wellness program required employees to complete both a confidential health risk assessment questionnaire and a confidential biometric screening. An employee, Bradley Seff, claimed that these requirements violated the ADAAA's prohibitions against required medical screenings. His claim resulted in a class-action lawsuit against the county.

The Court of Appeals affirmed the District Court's decision in favor of Broward County, finding that its wellness program fell within the ADAAA's safe harbor provision because it was a term of the County's benefit plan even though the wellness program was not a formal, written

---

[81] Peppet, *supra* note 4, at 125-126.

[82] Americans with Disabilities Act of 1990, as amended by ADA Amendments Act of 2008, 42 U.S.C. §12201(c)(1)-(3)(2008).

[83] *Id.* at (c)(3).

[84] Seff v. Broward County, Fla., 691 F.3d 1221 (11th Cir. 2012).

term of the County's plan.[85] Neither the District Court nor the Circuit Court addressed the question of whether the $20.00 surcharge for noncompliance in each pay period made the program involuntary. This precedent suggests that the ADAAA will not limit employers' ability to require employees to submit health and fitness data as a condition of employment.

3. The Electronic Communications Privacy Act

Another potential basis of legal protection is the Electronic Communications Privacy Act (ECPA), which makes it a crime to intercept or use electronic communications, but contains certain exceptions for employers.[86] It is unlikely that the ECPA would limit employers' use of health data collected from employees. One scholar, writing before health and fitness devices became common, concluded that the ECPA would not protect data contained in radio frequency identification (RFID) tags and read by RFID scanners.[87] He concluded that the transmitted data would not be an "electronic communication" within the scope of the ECPA. Another obstacle to using the ECPA in this context is that it 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."[88] Presumably both fitness devices like FitBits and fitness apps installed on mobile phones equipped with sensors, as most mobile phones are, would qualify as "tracking devices" and therefore fall outside the scope of the ECPA.

4. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act might also limit wearable device monitoring at work.[89] Although no court has yet determined whether a wearable fitness sensor qualifies as a "computer" within the meaning of the CFAA, relevant precedent suggests that a court would do so.

Under the CFAA, a computer is:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.[90]

When asked to determine whether a cell phone qualifies as a "computer" within the meaning of the CFAA, the Court of Appeals for the Eighth Circuit ruled that it did.[91] According to the Court, the CFAA's definition is "exceedingly broad" and "captures any device that makes use of a electronic data processor, examples of which are legion."[92] The rapid growth of technology, it noted, made it likely that more and more devices

---

[85] *Id.* at 1224.
[86] 18 U.S.C. § 2510-22 (1986).
[87] Lars S. Smith, *RFID and Other Embedded Technologies: Who Owns the Data?* 22 SANTA CLARA COMPUTER & HIGH TECH L.J. 695 (May 2006).
[88] *Id.* at 752-753, nn.285-287 (citing 18 U.S.C §§2510(12)(C), 3117(b) (2000)).
[89] 18 U.S.C. § 1030 (1986).
[90] 18 U.S.C. § 1030(e)(1).
[91] United States v. Kramer, 631 F.3d 900, 903 (8th Cir. 2011).
[92] *Id.* at 903.

would qualify as computers for CFAA purposes over time. "As technology continues to develop," said the Court, the CFAA's computer definition "may come to capture still additional devices that few industry experts, much less the Commission or Congress, could foresee."[93]

If employers access data from wearable devices or from the apps installed on their employees' mobile phones without employees' knowledge or permission, are they violating the CFAA? If the devices in question qualify as "computers" within the CFAA's "exceedingly broad" definition of that term, it would appear so. No court has yet addressed this specific question. Its resolution would likely depend in part on whether the employer had engaged in fraud or abuse in connection with those devices or apps, which presumably would depend on the validity and extent of employee consent to the monitoring. The more commonplace such monitoring becomes, however, the harder it will be for employees to prove a lack of at least implied consent.

C. There is No Effective Federal Agency Oversight of Employee Health and Fitness Data Collection.

Several government agencies might play a role in protecting health and fitness data from employer misuse. The FTC, the FDA and the Department of Health and Human Services (HHS), for example, may all have an interest in regulating this area.[94] This overlap of interests provides both an opportunity for interagency cooperation as well as a danger of overlapping and potentially inconsistent approaches to such regulation. As discussed above, however, HIPAA, the most relevant regulatory framework overseen by HHS, does not extend to employer's use of health and fitness data collected from most mobile devices and apps. The FDA is less concerned with the privacy implications of mobile technology than its effectiveness in improving health. The FTC is the most appropriate government agency to regulate the collection and use of employee health data, but serious questions remain about the effectiveness of its efforts in this area.

1. FDA Regulation

In January 2015, the Food and Drug Administration issued draft guidance on its plans to regulate certain "general wellness products," which may include fitness devices and software programs.[95] The FDA's guidance distinguishes between apps that effectively turn a mobile phone into a medical device and "general wellness products."[96]

---

[93] *Id.* at 903-904.

[94] *See, e.g.*, FEDERAL TRADE COMMISSION, INTERNET OF THINGS WORKSHOP, Remarks of Cora Han, *Internet of Things: Privacy and Security in a Connected World* (November 19, 2013), http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf at 165.

[95] *See* FOOD AND DRUG ADMINISTRATION, GENERAL WELLNESS POLICY FOR LOW RISK DEVICES, DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (January 20, 2015), http://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm429674.pdf. Covered devices "may include exercise equipment, audio recordings, video games, software programs4 and other products that are commonly, though not exclusively, available from retail establishments (including online retailers and distributors that offer software to be directly downloaded)." *Id.* at 2.

[96] FOOD AND DRUG ADMINISTRATION, MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (February 9, 2015),

Many of the health and fitness apps and devices that might transmit data of interest to employers fall into the FDA's "general wellness products" category. As illustrations of what might fall into this category, the FDA includes "a portable product that claims to monitor the pulse rate of users during exercise and hiking."[97] The FitBit might be an example. The FDA classifies this as a "general wellness product" because "claim relates only to exercise and hiking and does not refer to a disease or medical condition" and because "the technology for monitoring poses a low risk to the user's safety." Other examples of "general wellness products" include "a mobile application that solely monitors and records daily energy expenditure and cardiovascular workout activities to "allow awareness of one's exercise activities to improve or maintain good cardiovascular health" and "a mobile application [that] monitors and records food consumption to manage dietary activity for weight management and alert the user, healthcare provider, or family member of unhealthy dietary activity."[98]

The FDA suggests that it has no plans to regulate these "general wellness products."[99] The device and both kinds of apps that appear as examples of these products could generate data that an employer might intercept, but that is not the FDA's regulatory concern. Even if the FDA were to regulate these products, its primary concern would not be the potential for health and fitness data collection and sharing. The FDA's regulatory focus is the effectiveness and accuracy of these devices and apps rather than the privacy implications of their use.[100]

Some have called for the FDA to become more engaged in the regulation of mobile health and fitness technology.[101] Indeed, two weeks after its guidance on "general wellness devices," the FDA issued another draft guidance on "Mobile Medical Applications."[102] Recommendations include creating a new office for mobile medical technologies to educate consumers about apps that have health consequences for users and developing a requirement that app developers disclose the sources of medical information and calculations the app uses.[103] Its recent publications, however, suggest that the FDA will not take any significant role in monitoring or restricting the use of employees' health and fitness data in the workplace.

1. FTC Regulation

In its workshop on "The Internet of Things," the FTC devoted one of four panels to "Connected Health and Fitness," examining the "growth of increasingly connected medical devices and health and fitness products."[104]

In its report on that workshop, FTC staff recognized the danger that "unauthorized access to data collected by fitness and other devices that track consumers' location could endanger

---

http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf at 2.

[97] *See* FDA, *supra* note 95 at 7.

[98] *Id.* at 6.

[99] POLICY AND MEDICINE, FDA DEVICE GUIDANCE: GENERAL WELLNESS POLICY FOR LOW RISK DEVICES (January 29, 2015), http:// www.policymed.com/2015/01/fda-device-guidance-general-wellness-policy-for-low-risk-devices.html.

[100] *See* Hall, *supra* note 76, at 32.

[101] Nathaniel R. Carroll, *Mobile Medical App Regulation*, 7 ST. LOUIS U.J. HEALTH L. & POL'Y 415, 423 (June 2014).

[102] *See* FDA, *supra* note 96.

[103] *Id.*

[104] *See* FTC Staff Report, *supra* note 94, at 3.

consumers' physical safety."[105] A greater risk, however, is the danger that employers could use data collected by those devices to make adverse decisions about, and invade the privacy of, its employees. Scott Peppet, a participant in the workshop and a professor at the University of Colorado Law School, noted the potential dangers of using such data to make employment decisions at the workshop, but FTC staff declined to adopt his larger concern.[106]

D. Device Makers and App Developers Provide Too Little Information to Protect Employees from Data Misuse.

Can the health and fitness industry protect employee data well enough without regulatory intervention? Judging from the current state of the marketplace, I suspect not. The manufacturers of fitness devices that collect data currently face few restrictions on what data they can collect and how they can monetize it. Of course, sales from consumers provide one income stream, but downstream sales of data may be much more profitable. The potential profit from collecting, analyzing, repackaging and selling health-related data to employers and/or marketers is barely limited by law. As it stands, app and device makers can now access a wide range of users' health-related data without those users' consent.

Scholars are beginning to ask important questions about the extent to which app developers and device manufacturers must disclose their data collection and sharing practices. It can be hard for employees to find out how that personal health data is used or shared. Many health-related devices and apps lack clear indicia of what they may do with the data collected.

Providers pay at least lip service to protecting health-related data. In marketing its Health app, Apple reassures consumers that it takes their privacy concerns to heart:

> The information you generate about yourself is yours to use and share. You decide what information is placed in Health and which apps can access your data through the Health app. When your phone is locked with a passcode or Touch ID, all of your health and fitness data in the Health app is encrypted. You can back up data stored in the Health app to iCloud, where it is encrypted while in transit and at rest.[107]

There is a dichotomy, however, between industry assurances of consumer privacy and the rigors of the structures that would actually keep data private.

Apple encourages HealthKit developers to be transparent about their use of consumer data by asking them to "clearly disclose to the user how you and your app will use their HealthKit data."[108] This appears to be a suggestion rather than a contractual requirement. Apple itself distinguishes this and other "guidelines" from its "requirements," and urges HealthKit developers to make sure they comply with the latter.[109]

Apple does have contractual requirements regarding privacy that all app developers must follow, whether or not they use HealthKit.[110] According to them, the only apps that require a privacy policy are those that "collect, transmit, or have the capability to share personal

---

[105] *Id. at 13.*

[106] *See* FTC STAFF REPORT, *supra* note 94, at 169. For a more expansive discussion of these concerns, *see* Peppet, *supra* note 4.

[107] APPLE, INC., *Health. An Entirely New Way To Use Your Health and Fitness Information,* https://www.apple.com/ios/whats-new/health/.

[108] *See* THE HEALTHKIT FRAMEWORK, *supra* note 62.

[109] *Id.*

[110] APPLE, INC., *App Store Review Guidelines,* https://developer.apple.com/app-store/review/guidelines/, §17.

information […] from a minor" and those that "include account registration or access a user's existing account."[111] HealthKit developers are subject to the additional requirement that they "must provide a privacy policy," but Apple does not mandate the content, appearance or placement of such a policy.[112]

Apple also prohibits developers using the HealthKit framework from storing users' health information in iCloud and from using "data gathered from the HealthKit API for advertising or other use-based data mining purposes other than improving health, medical, and fitness management, or for the purpose of medical research."[113] Apple also notes that it will reject any app that "share[s] user data acquired via the HealthKit API with third parties without user consent."[114]

If an app developer were to violate these terms, however, it is not clear that the consumer whose data was sold would have a right of action against either Apple or the developer. Consumers may be incidental beneficiaries of these terms, but it is unlikely that a court would find that they had standing to sue either a developer for failing to follow them or Apple for failing to insist on them.

An alternative remedy could be to compel employers to disclose the extent to which they collect and use health data in employment decisions. It is hard to imagine how companies might be subjected to such a rule and how it might be enforced. As a further complication, it may be difficult to determine what impact, if any, health-related data may have on an employment decision ex post facto. Deciding what uses of health data are permissibly work-related may be especially challenging when the employer bears the cost of health insurance.

IV. Two Proposals to Restrict Employers' Misuse of Health Data

The lack of effective legal protection against the potential misuse of employee health data described in the preceding sections requires creative solutions. I propose two such solutions. One is designed to improve employee notice and decision-making about the disclosure of health and fitness data to employers by clarifying the terms and extent of such disclosure in advance. The other addresses the problem from the employer's end by limiting the potential collection and use of that data.

A. The FTC Should Require Standardized, Succinct Privacy Labels on Health and Fitness Apps and Devices.

An important regulatory question is the extent to which app makers should be required to provide clear information about their privacy policies as a condition of use. My first recommendation is the implementation of a mandatory labeling regime for all apps and devices that collect health-related information. The labeling proposed here would provide all consumers, including the employees that are the focus of my concern in this article, with a more realistic and practical means of limiting access than they currently have.

---

[111] *Id.* at §§17.4 and 17.5.
[112] *Id.* at §27.7.
[113] *Id.*
[114] *Id.*

1. Current Website Privacy Policy Requirements Suffer From Three Critical Deficiencies.

A privacy labeling rule would correct many of the deficiencies from which current privacy policies suffer. While websites are currently required to have privacy notices, these notices are not an effective means of providing employees with meaningful choice about how their data would be shared. There are at least three problems with privacy policies as they currently appear on health and fitness-related websites. First, it can be hard to locate them, especially on multi-page websites. Second, they are difficult and time-consuming to read. Third, they have inconsistent terms and scopes, making it hard to compare their practices.

Legal scholars have pointed out that a major problem with the privacy notices associated with health and fitness devices is that they are hard to find.[115] Professor Peppet describes his experience of opening a Breathometer device he had purchased which measures blood alcohol content. The device came with a seventeen-page manual for using the device and opening the associated app, but the manual made no mention of a privacy policy. [116] Nor did the app itself when installed or the device upon startup. Nothing in the device, app or manual disclosed whether the device collected any data other than blood alcohol content test results. It did not disclose how any collected data might be stored, transferred, sold or deleted. "Only by visiting the company's website, scrolling to the very bottom, and clicking the small link for 'Privacy Policy,'" Professor Peppet writes, "can one learn that one's blood-alcohol test results are being stored indefinitely in the cloud, cannot be deleted by the user, may be disclosed in a court proceeding if necessary, and may be used to tailor advertisements at the company's discretion."[117] One can only imagine what kind of advertisements those might be.

Not all health related data collectors provide even this much information. Software manufacturer Welbe, whose products allow employers to aggregate employee health data from various sources, offers even less information about its privacy filters to the public. On its website, one has to scroll all the way to the bottom of the screen to find a small link called "Privacy Policy."[118] Clicking on that link brings up the "O.C. Tanner Company Privacy Policy," which applies to all websites operated by what is apparently WelBe's parent company rather than to the WelBe products themselves.[119]

A second problem is that it takes an unreasonably long time to read the notices once they are found. By one account, if someone were to read the privacy policy on every website she visits at least once a year, she would spend approximately 244 hours a year reading privacy policies.[120] Most privacy policies are cumbersome and difficult to interpret. The FTC itself has criticized the effectiveness of industry-generated privacy notices, observing that "the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand."[121] It is unrealistic to expect lengthy,

---

[115] *See* Peppet, *supra* note 4.
[116] *Id.*
[117] *Id.* at 90.
[118] *See* WELBE, *supra* note 58.
[119] O.C. Tanner Privacy Policy, *available at* https://www.awardselect.com/privacy/p_en_US.html.
[120] Aleecia M. McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies***,** 4 ISJLP 543, 560 (2008).
[121] Press Release, Fed. Trade Comm'n, *FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses and Policymakers* (Dec. 1, 2010), *available at* www.ftc.gov/news-events/press-releases/2010/12/ftc-staff-issues-privacy-report-offers-framework-consumers.

obscure policy notices to provide the kind of meaningful choice that consumers want and that privacy legislation aims to provide.

Privacy policies may vary widely in substance, even when such policies are required. Recognizing that consumers may have concerns about the privacy of their health data, Apple notes that "apps that access HealthKit are required to have a privacy policy," although it does not mandate the specific parameters of the policy.[122] In its instructions for developers, Apple refers them to two government websites for "guidance."[123] One is a "Personal Health Record model (for non-HIPAA apps)," which links to the HealthIT's suggestions for a model privacy notice.[124] The other site is described as the "HIPAA model (for HIPAA covered apps" and links to the Office of Health and Human Services privacy notice rules.[125] Apple does not, however, help developers determine whether their products are covered by HIPAA or not, and consequently which set of guidelines they should follow.

2. Industry Self-Regulation of Privacy Policies Has Failed, Making Legislative Intervention Necessary.

Consumer products sold in the United States are required to carry warranties that meet certain legibility requirements, pursuant to the Magnuson-Moss Warranty Act.[126] In passing that Act, Congress intended to make sure that consumers could get complete information about warranty terms and conditions, thereby helping them to make more informed purchases.[127] The Magnuson-Moss Warranty Act also allows consumers to compare warranty coverage among products before buying and promote competition on the basis of warranty coverage. By clarifying the sellers' obligations, the Act also makes it easier for consumers to pursue a remedy for breach of warranty in the courts.

One could argue that the same policy concerns underlie the need for clear data disclosure policies. Why should data disclosure policies be more difficult to discern than warranties? The potential losses consumers could suffer as a result of the unauthorized use of their data – especially the health-related data that arguably would be protected under HIPAA if it were used by "covered entities" – could well exceed the potential financial losses that the Magnuson-Moss Warranty Act sought to limit.

The Federal Trade Commission appeared to be moving toward just such a labeling requirement when its Chairman Jon Leibowitz announced, in 2012, plans to develop what it called a "Privacy Nutrition Label" for data collection and use[128] As envisioned at the time, this label would have contained "five essential terms" related to privacy, although the FTC was still in the process of identifying those terms in conjunction with the Bureau of Consumer Protection. The FTC had considered adopting some form of standardized privacy labels, modeled after

---

[122] *See* THE HEALTHKIT FRAMEWORK, *supra* note 62.
[123] *See supra*, note 107.
[124] *Id.*
[125] *Id.*
[126] 15 U.S.C §2301 et seq. (1975).
[127] FEDERAL TRADE COMMISSION, *Businessperson's Guide to Federal Warranty Law*, http://www.ftc.gov/tips-advice/business-center/guidance/businesspersons-guide-federal-warranty-law.
[128] Josephine Liu, *FTC Working on Privacy "Nutrition Label"; Industry Focusing on Icons*, (October 25, 2012), http://www.insideprivacy.com/united-states/federal-trade-commission/ftc-working-on-privacy-nutrition-label-industry-focusing-on-icons/.

nutrition labels, as early as July 2001.[129] Since Leibowitz resigned from the FTC in 2013, however, there has been no further mention of government-mandated privacy labels for apps.

There is an apt analogy in product labeling laws, including the food labeling laws Congress has passed in recent years. Beginning in the early 20th century, certain furniture and bedding makers were required to label their products so that the public would know what materials were used inside (e.g., horse hair).[130] The Food and Drug Administration enforces a complex series of food labeling laws that apply to all food products sold in the United States.[131]

Labeling requirements have continued to evolve and extend in response to social changes. In late 2014, noting that Americans now "eat and drink about one-third of their calories away from home," the FDA announced new labeling rules that require certain restaurant chains to label menu items with nutritional information and all vending machines to provide calorie count labels for each item sold.[132] The rules extend nutrition label requirements in order to "help consumers make informed choices for themselves and their families."[133]

If the FDA can adapt labeling requirements to help consumers make more informed choices, it stands to reason that the FTC can develop privacy label requirements for health-related devices and apps for the same purpose. Although food consumption and data disclosure differ in some key ways, mandating the provision of more information about each can only help the consumer.

In its 2015 report on the Internet of Things, the FTC agreed that "[w]hatever approach a company decides to take, the privacy choices it offers should be clear and prominent, and not buried within lengthy documents."[134]

There has been extensive research on the best formats for privacy nutrition labels already. Researchers at Carnegie Mellon and other universities have developed privacy labels that indicate, at a glance, how a provider might use or share each of several kinds of information.[135] Here is a sample of such a label:

---

[129] *Id.*

[130] *See* http://www.americanlawlabel.com/law-label-learning-center/#products

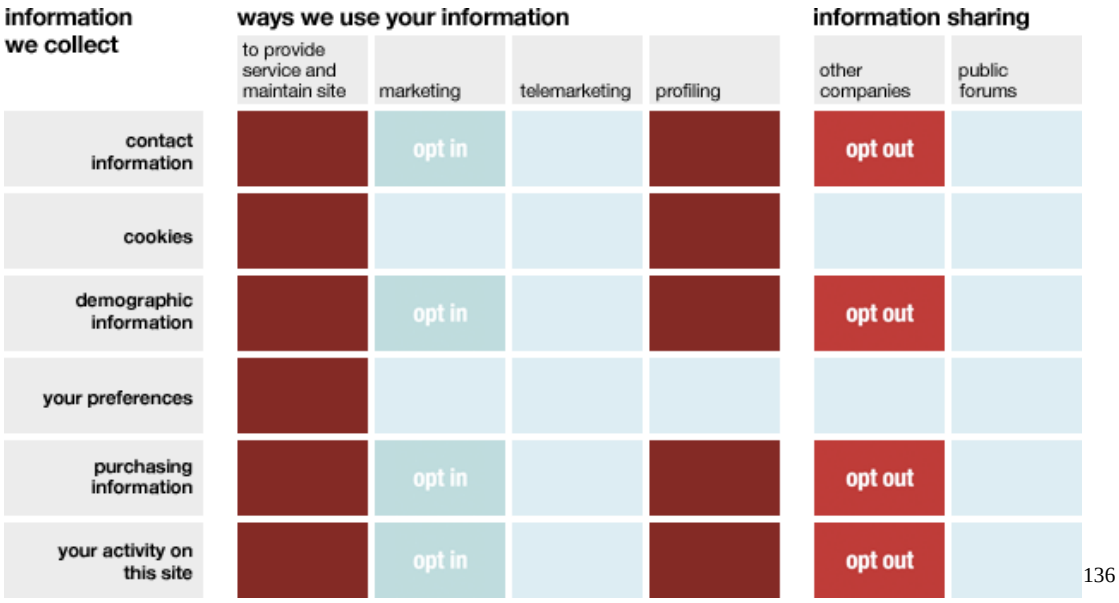
[131] *See, e.g.*, 21 C.F.R. §101 et seq.

[132] *See* U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, FOOD AND DRUG ADMINISTRATION, MENU AND VENDING MACHINES LABELING REQUIREMENTS, http://www.fda.gov/Food/IngredientsPackagingLabeling/LabelingNutrition/ucm217762.htm.

[133] *See* U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, FOOD AND DRUG ADMINISTRATION, OVERVIEW OF FDA LABELING REQUIREMENTS FOR RESTAURANTS, SIMILAR RETAIL FOOD ESTABLISHMENTS AND VENDING MACHINES, http://www.fda.gov/Food/IngredientsPackagingLabeling/LabelingNutrition/ucm248732.htm.

[134] *See* FTC STAFF REPORT, *supra* note 94, at v.

[135] *See, e.g.*, Cylab Usable Privacy and Security Laboratory, Carnegie Mellon University, *Privacy Nutrition Labels*, http://cups.cs.cmu.edu/privacyLabel/; Patrick Gage Kelley et al, *A Nutrition Label for Privacy*, http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf; *see also* Kleimann Communication Group, Inc. *Evolution of a Prototype Financial Privacy Notice*, (February 28, 2006), *available at* https://www.ftc.gov/sites/default/files/documents/reports/evolution-prototype-financial-privacy-notice.pdf.



[136]

By providing standardized labels that are easy both to read and compare, providers would make it easier for consumers to make meaningful choices about the data they share. Apps and devices should be required to carry concise, effective privacy labels for this purpose. The privacy nutrition labels developed by the CUPS program at Carnegie Mellon University, led by Lorrie Faith Cranor, provide an excellent starting point.[137]

While the CUPS model should serve as a starting point, I recommend two improvements for the legal community's consideration. First, the standard data privacy label as it appears on websites should allow employees to click directly on the provisions to opt out of each kind of disclosure. The labels' original architects envisioned this kind of opt-out provision, but could not implement it when it was introduced due to a lack of standards for opt-out mechanisms.[138]

Second, a graphic version of this label should appear on the external packaging of all wearable fitness devices, just as nutrition labels must appear on the outside of packaged food sold in the United States. In a survey of twenty popular Internet of Things consumer devices, not one of them included privacy indicia on the box.[139] The provision of an external, easy to read label, accessible to the consumer before the purchase, will help inform and improve purchasing decisions about products that can collect and share health data.

3. The Benefits of Mandatory Privacy Labels Will Outweigh The Costs.

---

[136] *See* http://cups.cs.cmu.edu/privacylabel-05-2009/current/1.php. Reprinted with the kind permission of Lorrie Cranor, Associate Professor, Computer Science and Engineering & Public Policy and Director, CyLab Usable Privacy and Security Laboratory at Carnegie Mellon University.

[137] Other privacy label ideas have been proposed as well, such as Aza Raskin's development of a set of privacy icons at Mozilla. *See, e.g.*, Aza Raskin, *Privacy Icons: Alpha Release* (Dec. 27, 2010), www.azaraskin/blog/post/privacy-icons/.

[138] Lorrie Faith Cranor. *Necessary But Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, 10 J. ON TELECOMM AND HIGH TECH L. 273, 289-290 (2012).

[139] *See* Peppet**,** *supra* note 4, at 141. In fact, none of the surveyed devices made reference to a privacy policy on an associated website anywhere in the packaging materials or user guides. *Id.*

A leading scholar in this area suggests that regulators "seek industry consensus on best practices for where and when to give consumers notice about privacy and data issues."[140] I respectfully disagree. Suggesting new legislative remedies in scholarly articles is often seen as too cumbersome to be realistic. In this case, however, a legislative remedy may be the only realistic way to improve the protection of health-related data in the employment context. Voluntary programs to develop data privacy disclosures have done little to improve consumer or employee protection. Recommendations that rely on industry to make it easier for consumers to limit the data that industry potentially can sell have, perhaps unsurprisingly, failed repeatedly over the last two decades. One scholar notes that the state of privacy protections in 2012 closely resembled the state of such protections in 1996, when commentators first launched efforts to standardize website privacy practices.[141] According to her, "The experience over the past fifteen years demonstrates that privacy user empowerment tool and notice and choice mechanisms are insufficient to protect privacy.[…][E]nforcement mechanisms are needed to ensure that users' choices are respected."[142]

Another benefit of legislation is the corresponding enforcement power. Enforcement presumably would address not only the provision of privacy labels but their accuracy as well. There is reason to suspect that app developers and website providers might misrepresent their practices absent such enforcement. Scholars found that websites voluntarily posting privacy policies in order to comply with an earlier web standard, Platform for Privacy Preferences, frequently misrepresented their privacy policies in order to get more favorable placement within the web browser Internet Explorer.[143] While consumers could also sue providers for fraud, the potential costs of doing so and problems of quantifying injury from invasions of privacy may deter that kind of litigation.[144]

Some scholars have noted that industry is unlikely to develop more effective privacy notice and choice policies unless there is an incentive to do so.[145] For the reasons described above, I believe that the carrot is insufficient, and the stick is needed.

Developing a labeling requirement like this will pose challenges. None of these challenges outweigh the significant benefits that a privacy labeling program would provide.

One problem in implementing such a privacy label is that there is already a competing, although not mandatory, privacy labeling regime. The Office of the National Coordinator for Health Information Technology has established a Personal Health Record (PHR) Model Privacy Notice. Its goal is to provide a template that a "web-based PHR company can use to succinctly inform consumers about its privacy and security policies."[146] By its terms, the PHR Model Privacy Notice is not required of companies that collect health data online, although it was

---

[140] *Id.* at 163.
[141] *See* Cranor, *supra* note 138, at 276.
[142] *Id.* at 304-305**.**
[143] Pedro Giovanni et al., *Token Attempt: The Misrepresentation of Website Privacy Policies through the Misuse of P3P Compact Policy Tokens, 4 Workshop on Privacy in the Electronic Society* (Sept. 10, 2010), *available at* www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab10014.pdf.
[144] In December 2011, a judge dismissed a class action against Amazon for misrepresenting privacy policies because the plaintiffs failed to allege the minimum financial harm required with sufficient specificity. Venkat Balasubramani, *The Cookie Crumbles for Amazon Privacy Plaintiffs*, TECHNOLOGY & MARKETING LAW BLOG (December 2, 2011), http://blog.ericgoldman.org/archives/2011/12/the_cookie_crum.htm.
[145] *See* Cranor, *supra* note 138, **at ___ [Liz to find page]**
[146] HEALTHIT.GOV, *Personal Health Record (PHR) Model Privacy Notice*, http://www.healthit.gov/policy-researchers-implementers/personal-health-record-phr-model-privacy-notice.

apparently inspired by mandatory labeling regimes.[147] Like the CUPS label, the PHR Model Privacy Notice "is meant to be similar to other consumer-oriented 'labels' that have been developed for other industries, such as the nutrition facts label for food and the Model Privacy Notice developed for the financial services industry for compliance with the Gramm-Leach Bliley Act."[148]

Another challenge of such a regime is that the additional labeling may add cost, which ultimately will be passed on to the purchaser. The cost of changing product packaging to include standardized packaging labels is likely to be minimal, however, especially relative to the cost of consumer electronics. Since every product will bear the same cost, no provider will be at a competitive advantage or disadvantage vis a vis these costs. Finally, research has shown that consumers are willing to pay a bit more to buy goods from more secure sites when they were given information about how the sites shared their data.[149]

Reaching consensus on a privacy labeling regime may be difficult. Several federal agencies are likely to play some role in developing such a regime, which therefore will require inter-agency collaboration. There is precedent, however, for multiple government agencies working together to develop a comparable labeling requirement. In order to develop the model privacy notice that the Gramm-Leach-Bliley Act requires financial organizations to send to their customers, eight government entities collaborated and jointly announced the final model notice.[150] If those entities can work together to develop a model notice (which took the form of a table), then there is reason to believe that the FTC, the FCC, the FDA and other interested agencies will be able to cooperate on a model health data privacy label. The FTC's leadership on this issue may also facilitate interagency cooperation. While other agencies have an interest in the development of privacy labels and should be consulted, the FTC has the clearest mandate both to lead the regulation and to enforce it.

A final shortcoming of this solution is that it does little to address the concerns of employees who are required to wear health and fitness sensors, and therefore have limited choice in the devices they use. Improving the information available to them about the monitoring systems used, however, will make these practices more transparent.

B. Extend HIPAA's Definition of Covered Entities to Include Employers, App Developers and Wearable Device Manufacturers.

My second recommendation would restrict employers' use of health and fitness data more than federal laws currently do. While I believe that a legislative solution is necessary for reasons I describe below, I do not propose entirely new legislation to curtail the use of this data.

---

[147] The Office of the National Coordinator for Health Information Technology, HEALTHIT.GOV, *About the PHR Model Privacy Notice: Background, Development Process and Key Points* (September 2011), http://www.healthit.gov/sites/default/files/phr-model-privacy-notice-backgrounder-final.pdf at 2 ("Like the FDA nutrition facts label, the Model Notice is intended to enable companies to present complex information in a manner that is accessible, consistent, and conducive to informed choice. Unlike the FDA nutrition facts label, use of the Model Notice is voluntary.")

[148] *Id*.

[149] *See* Cranor, *supra* note 138, at 292-293.

[150] These were the Federal Reserve Board, the Office of Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, the Federal Trade Commission, the Securities and Exchange Commission, and the Commodity Futures Trading Commission. *See* http://files.consumerfinance.gov/f/201410_cfpb_final-rule_annual-privacy-notice.pdf at 3-4.

A regulatory structure is already in place for the protection of health-related data in the form of HIPAA. As discussed above, the current definition of "covered entities" under HIPAA excludes employers, device manufacturers and app developers. Revising the definition of "covered entities" to include them would extend the protection that employees have come to expect of their health-related data to more of the entities that could misuse that data. Similarly, expanding the definition of "[i]ndividually identifiable health information" to data generated by mobile health and fitness sensors including those built into mobile phones as well as dedicated fitness devices would bring more of this data within the scope of HIPAA protection.

Much of the administrative framework that would be needed to protect employee health and fitness data also exists in HIPAA. The Security Rule, for example, specifies steps that covered entities must take to ensure the confidentiality and integrity of electronic personal health information.[151] It also protects against the uses and disclosure of such information.[152] In fact, the HIPAA Security Rule is one of the most detailed and prescriptive of all United States information security laws.[153]

The HITECH rules that amend existing HIPAA obligations provide sufficient coverage to extend the protection of data to entities that work with employers, for example, by collecting or interpreting employee health data for those employers. Under the HITECH rules, such entities may be considered Business Associates and therefore be subject to certain restrictions on the use and transfer of personal data.[154]

C. Securing Employee Health Data Requires Additional Study and Discussion.

Neither of the two solutions I propose here is sufficient, either alone or in combination with the other, for the complete protection of personal health-related data from potential employer misuse. These two suggestions will not resolve all of the legal and ethical problems concerning employers' acquisition of employees' health and fitness data described in this article. For example, if the FTC were to require privacy nutrition labels like the ones suggested here, there presumably would be no private right of action. Employees whose health and fitness data was shared in a manner inconsistent with the privacy product labeling could not seek redress directly from the manufacturer or developer, but would instead have to rely on the FTC to enforce its directives. If the FTC were to decline enforcement for any reason, the employee would have no remedy against the manufacturer or employer. In addition, neither of the solutions I propose resolves the underlying problem of potential vagueness as to what constitutes protectable information.

The legality of health data privacy at work should also be part of a larger discussion about the modern value of privacy in general. As Kate Murphy wrote in a widely shared New York Times essay, people both value privacy and cannot seem to stop sharing information.[155] As Murphy noted, a three-year German study showed a privacy paradox in that the more people

---

[151] HIPAA Security Rule, 45 C.F.R. §§ 160 and 164(A) and (C) (2003).
[152] HIPAA Privacy Rule, 45 C.F.R. §§ 160 and 164(A) and (E) (2003).
[153] Getting The Deal Through, *Data Protection and Privacy in 26 Jurisdictions Worldwide 2014*, (Rosemary P. Jay, contrib. ed.), *available at* http://www.gtlaw.com.au/wp-content/uploads/Australia-GTDT-Data-Protection-Privacy-2014.pdf.
[154] 78 Fed. Reg. 5566 (Jan. 25, 2013), amending 45 C.F.R §§ 160, 162, 163 and 164.
[155] *See* Murphy, *supra* note 73.

disclose about themselves, at least on social media, the more privacy they desire.[156] While there may be a benefit to measuring the biometric data of workers, employers risk sacrificing the quality of their work. According to Murphy,

> Privacy research in both online and offline environments has shown that just the perception, let alone the reality, of being watched results in feelings of low self-esteem, depression and anxiety. Whether observed by a supervisor at work or Facebook friends, people are inclined to conform and demonstrate less individuality and creativity. Their performance of tasks suffers and they have elevated pulse rates and levels of stress hormones.[157]

These studies have another implication that employers should value. They suggest that performance suffers when employees experience a loss of privacy. Of course, employers need to monitor their employees to a certain extent as they have always done. What this research suggests, however, is that an increase in biometric and health data collection may correlate with a decrease in work performance quality.

V. Conclusion

Health data collected from wearable technology may affect employment decisions and status in ways that U.S. law has never before permitted. Business analysts predict that the amount of employee-generated health and fitness data will rise exponentially over the next several years. At the same time, employers' ability to collect, analyze and act on that data is essentially unfettered by law. Employers have every incentive to use that data for a variety of purposes. Many of them are finding new ways to do so now, aided by insurers and data providers.

Employees have little legal protection from employment practices that hinge on access to their health and fitness data. While the use of this data may be risky for the monitored employees, there may be no federal basis of liability for employers for any consequent harm. Employees therefore face a growing risk, with no clear legal remedy. While the legal risks associated with employer use and collection of employee health and fitness data are starting to attract scholarly attention, better solutions are needed. In this article, I have proposed two specific solutions that would offer monitored employees more notice, choice and remedy regarding these practices. A mandatory privacy labeling law for fitness devices and health-related apps would help employees to better understand the health data that employers can access from their use. Extending the terms of HIPAA to cover employers as well as medical professionals, and health and fitness data generated from popular mobile sensors as well as more traditional medical records, would align expectations of health privacy with a legal right to that privacy. While neither solution is perfect, they provide a basis for further discussion of the best ways to address this growing problem.

---

[156] PRIVACY ONLINE: PERSPECTIVES ON PRIVACY AND SELF-DISCLOSURE IN THE SOCIAL WEB, (Sabine Trepte and Leonard Reinecke, eds. 2012), http://www.springer.com/us/book/9783642215209.

[157] *See* Raskin, *supra*, note 137.