Ryan McErlean
Professor Ricciardi, Senior Capstone
First Draft

May 3, 2017

Fitbits & Employee Health Data: Privacy, Protection, and Gaps in the Law

Part I: Introduction

In today's digital age, technology has grown at a faster pace than the law. The amount of data being shared between consumers at any given time is alarming, leaving them defenseless over breaches in privacy in many forms. Unfortunately, most users are ignorant of the magnitude of what such breaches can entail. It has been shown that as technology grows and new products are released to the market, consumers' expectations of privacy have decreased. However, this decrease is likely due to the fact that consumers simply do not realize what this lack of privacy can mean for them.

One area that is particularly concerning is consumer health data and the potential for misuse. Moreover, there is a growing trend for employers to incorporate wearable devices such as the Fitbit into their wellness programs and health insurance policies. To employees, this may seem like an innocuous win-win situation. However, these arrangements provide employers with more health information on their employees than ever before. More importantly, the law currently does not protect or even mention employer misuse of health data. Hirings, firings, promotion decisions, and discrimination are just a few of the types of decisions employers can make based on their employees' health information. Wearable devices such as the Fitbit give employers free reign to do with this data as they wish. Without legal protection of their personal information,

employees will remain vulnerable to countless unethical uses of it at the workplace. Until existing law is extended, or new policies are implemented, the misuse of employee health data at the workplace will persist and likely worsen.

Part II: Background Information: Fitbits, the Internet of Things, and Corporate Wellness Programs

In recent years, the popularity of wearable technology has increased significantly. Industry leader Fitbit has become synonymous with the wearable technology movement. With the purchase of a Fitbit, consumers can track and monitor their health data by wearing the watch-like wrist band everywhere they go. The company asserts that purchasing a Fitbit can help customers improve their health by making positive lifestyle changes. However, a number of privacy issues have risen regarding the data stored in Fitbits and similar wearable devices. Employers have grown increasingly interested in tracking their employees' health information, and some are now using Fitbits to do so. Before discussing the legal issues of Fitbits at the workplace, it is important to understand exactly what Fitbits are, and why the data stored in them could be valuable to employers.

In 2007, Fitbit was first launched in San Francisco. The company currently sells seven wearable devices, a wireless "smart scale" called the Aria, and several Fitbit accessories.[1] According to their website, "Fitbit motivates you to reach your health and fitness goals by tracking your activity, exercise, sleep, weight, and more."[2] Once a Fitbit

---

[1] Fitbit

[2] Ibid.

is purchased, the customer is required to set up a Fitbit account on their phone, computer, or both. Once the customer begins to wear the Fitbit, all the data it stores is transferred and synced to their computer or mobile device. This data includes heart rate, steps walked, stairs climbed, quality of sleep, GPS, calories burned, weight, and food consumption. Some of this data, such as weight and food consumption, requires the user to manually enter the information into their phone or computer. If the customer owns a Fitbit Aria scale, their weight will be synced automatically. Users can set goals, track their progress, and observe short and long term health patterns with their Fitbits. If desired, Fitbit users can also share this data directly with friends and set up group activities with their Fitbit accounts. At the end of 2016, Fitbit reported that it had 23.2 million active users, with 50.2 million total registered users.[3] In summary, Fitbits store a huge amount of health information of a growing number of consumers.

Due to Fitbit's WiFi and bluetooth accessibility, along with built GPS tracking, it falls within the Internet of Things. The Internet of Things is an umbrella term describing the growing interconnectivity of common electronic devices. Examples include smartphones, cars, computers, headphones, home appliances, smart TVs, and of course wearable fitness devices such as the Fitbit. It is now possible to monitor one's laundry, home security, lights, and health data from smartphone applications using WiFi and bluetooth. Estimates suggest that by 2020, the Internet of Things will include 200 billion devices with a market size of roughly $2.7 trillion.[4] Such devices offer countless benefits and conveniences, but they also share a great deal of information. In a public

---

[3] Fitbit, as quoted in Business Wire.

[4] Peppet, 3.

Wi-fi network, dozens of smartphones, computers, and other devices share information and data with each other. Security measures have not sped up to the production of such gadgets, and most consumers are unaware of this fact. Questions arise as to who owns the data, how it may be used, and who can see it. As the Internet of Things grows rapidly, so do the ease and potential for security breaches and hacks. In December 2015, a large Fitbit security breach left users vulnerable to the sharing of their personal information.[5] The functionality of the Fitbit invariably places it with the Internet of Things. At the workplace, the Fitbit transmits information in the same manner as it does in public or private places.

While Fitbits were originally intended for personal use by an individual, a growing number of companies are becoming interested in using Fitbits at the workplace. Fitbit now offers Fitbit Wellness, a group health initiative that may be used by employers for their company. Fitbit's website claims that group packages can increase engagement and improve work performance as a result of better health. Fitbit Wellness also allows employees to enter "team challenges" and compare results with their co-workers, all of which is monitored by their employers. In many cases, employees are offered reduced health insurance costs for being in good health. Employers can get significant discounts for health insurance policies when they can prove that most of their employees are in good health. To prove this, companies can now use Fitbits to track and present employee health information to insurance companies. In 2015, Fitbit CEO James Park stated that while corporate services accounted for under 10% of the company's

---

[5] Levy, 1.

revenue, it is “one of the fastest-growing parts of the business.”[6] It is important to note that employers may use Fitbits at the workplace without using Fitbit Wellness, however it makes the process easier for them. Additionally, corporate wellness programs and health insurance policies may include other methods of data collection, and will be discussed in Part III. These issues are also not exclusive to Fitbits, as the exact same issues exist with similar devices.

Corporate packages are seen as a “win-win” for both employees and employers. In recent years, companies have increased focus on their wellness programs, and spending on these initiatives has more than doubled since 2009.[7] About 90% of companies offered wellness programs in 2016 according to the *Harvard Business Review.*[8] Such programs, many of which now use the Fitbit, promote better health, camaraderie, and higher production in the workplace. One example is BP, where employees who participate in the program collect points through documented completion of a variety of activities. In 2016, some examples were completing the “Million Step Challenge,” attending their annual physical exam, or taking an on-site biometric employee screening.[9] Employees who completed the Million Step Challenge earned 500 points, half of the amount needed annually to qualify for health care reductions.[10] In 2014, such reductions could reach $1200 or more for participating BP

---

[6] Seitz, 1.

[7] Satariano, 1.

[8] Fort, 8.

[9] BP Human Resources, 2.

[10] Satariano, 1.

employees.[11] Located in the San Francisco Bay area, software startup Appirio has benefitted financially from sharing employee data with its insurance provider. By offering Fitbits to employees and collecting their health data, the company showed that employee health was improving, and reduced its $5,000,000 annual insurance costs by $300,000.[12] Other companies that have adopted similar wellness plans using Fitbit or other wearable devices include Target, Bank of America, and Time Warner.[13]

In most cases, participation in such wellness programs remains voluntary for employees. However, starting in 2013, CVS has taken a more stringent approach in gathering employee health data. Though the company has not incorporated Fitbits or other wearables into their program, they require that all employees using its health plan directly provide information including weight, glucose levels, and body fat.[14] While CVS claims that its plan is voluntary, any employees who fail to report such information are fined $50 each month, or $600 annually.[15] Another example is Walmart, which hires a third party wellness program vendor called Castlight. Health data from all Walmart employees is collected by Castlight and presented to Walmart executives. Along with employee search engine history, the data can be used to reach significant conclusions including risk level for diabetes or pregnancy for female employees. Employees may then be sent messages directly regarding weight loss suggestions or prenatal health

---

[11] Brown, 6.

[12] Ibid, 6.

[13] Chen, 1.

[14] Brown, 2.

[15] Ibid, 2.

information based on these conclusions.[16] Although CVS and Walmart do not use Fitbits or similar devices to gather its data, their practices illustrate the growing level of interest and value in employee health information.

The Fitbit is certainly an effective tool in monitoring one's personal health. When discussing employee privacy issues regarding the Fitbit, it is important to first look at the the issue from a variety of angles. The Fitbit stores a large amount of personal health information for those who use it. Such data is becoming increasingly accessible with the rapid growth of the Internet of Things, and law has not caught up with the phenomenon. Employers have taken notice of the value of such data, and are going to greater lengths to acquire it. At a first look, these wellness programs often seem benign and well intended, and many of them certainly are. However, the companies have a vested interest in their employees' health data, and how it is used can raise a number of privacy questions. Unfortunately, the law currently does little to restrict employers from making unethical decisions with employee health data.

Part III: Current Law Fails to Define and Protect Employer Misuse of Employee Health Data

It is evident that there is ample opportunity for employers to misuse employee health data, whether it is collected from wearable devices like the Fitbit or otherwise. The reason for this is that federal law does not adequately protect employee health data. Though there are current acts and laws in place that may pertain to the issue, they can only be vaguely applied, and are mostly insufficient to protect employees. Examples include the Health Insurance Portability and Accountability Act (HIPAA) and the

---

[16] Ajunwa, 2.

Americans with Disabilities Act Amendments Act (ADAAA). While one would imagine that private employee health and/or fitness information would be protected under these laws, neither of them address the issue explicitly. Moreover, no federal agency is officially responsible for regulating the collection of employee health data. Without any concrete representation by the government or federal law, the problem is essentially lost in the shuffle. Regardless of how unethical it may seem to misuse an employee's health data, the courts must make decisions based on the law. Until new laws are created or old ones revised, employees will remain vulnerable and unprotected in the use of their personal health and fitness information.

Information collected by a FitBit, or even a smartphone sensor, can tell employers a lot about their employees. In his article discussing the Internet of Things, Professor Scott R. Peppet states that

> researchers are beginning to show that existing smartphone sensors can be used to 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 of physical activity or movement. [17]

Here, though he is discussing smartphone sensors specifically, this information applies to Fitbits, which would arguably provide even more accurate data. To conclude that an employee may be bipolar based on health data collected by a sensor would sound outlandish, even impossible, to the average person. This may seem like an extreme and unlikely scenario, but the truth is that it is now possible with technology. In reality, the more benign seeming examples such as sleeping patterns, heart rate, and stress levels can suggest quite a lot about an employee. In particular, Fitbit users may also enter

---

[17] Peppet, 14.

data such as caloric intake, blood sugar levels, exact foods consumed, and hydration levels into their mobile application. With this information, employers can speculate the probability of an employee having health issues in the future, and make promotion or hiring decisions based off of it. Because the employee does not yet have the health condition, they are not considered to have a disability, and are not protected by the law.[18] Many employees are unaware of these potential misuses of their personal data, and most are unlikely to consider it when they agree to use wearable devices through their workplace. Until the law catches up to technology, this ethical gray area will persist.

Currently, there are a number of laws and acts that could arguably address the issue of employee health data protection. Though the act was itself created to protect the privacy of patients, HIPAA does not cover health information gathered by wearable devices such as the Fitbit.[19] Specifics such as heart rate, sleeping patterns, and calorie consumption remain unprotected by the act.[20] Another important shortcoming of HIPAA is that any data collected by a third party, which would include an app developer used by Fitbit, is not protected.[21] In other words, if a company signs up for Fitbit Wellness, Fitbit takes care of monitoring, tracking, and storing all of the employee health and fitness information. So any data that the company receives directly from Fitbit is not covered by HIPAA. Even if the company uses Fitbits without Fitbit Wellness, the health information collected from the employees' Fitbits is not protected in the first place.

---

[18] Peppet, 17.

[19] 45 C.F.R § 160.103

[20] Brown, 9.

[21] Ibid, 9.

Though there are some parts of HIPAA that could arguably refer to employee health data, they don't mention it explicitly. This essentially leaves employees' personal health information as "fair game" for employers to use.

Another example to consider is the ADAAA, which is an edited version of the Americans with Disabilities Act. The expansion was made to further protect employees' rights at their workplace. In her article on the ethical issues of Fitbits at the workplace, Professor Elizabeth Brown says,

> The Americans with Disabilities Act Amendments Act (ADAAA) expands the ADA's protections against employment discrimination on the basis of an actual or perceived disability. Much of the fitness data that sensors generate and employers collect, however, neither constitutes nor correlates with a disability as defined under the ADAAA. [22]

Here, Brown discusses how both the act itself and the amendment act are insufficient to protect employee health data. However, the ADAAA was used in a similar case that did not involve wearable devices. In Seff v. Broward County, employee Bradley Self sued his employer (Broward County) for deducting $20 from his paychecks for refusing to participate in biometric health screenings for the insurance policy. The biometric screenings consisted of an online questionnaire and a finger prick that tested for both glucose and cholesterol levels. The county argued that technically, these tests were not mandatory to receive health insurance. However, any employees that used its insurance and did not participate, including Seff, were charged $20 from each paycheck. In Seff's appeal, the US Court of Appeals for the Eleventh Circuit held the decision in favor of Broward County. The reasoning for this was based on the ADA's safe harbor provision, which exempt Broward County from the Act's banning of involuntary medical

---

[22] Ibid, 10-11.

examinations from employers.[23] Essentially, the county was not found guilty of breaking the law based on a loophole of the ADAAA. Though this case does not involve Fitbits or other wearables, it's relevant because it deals with the same health data that these devices provide to an employer. Similarly to HIPAA, the ADAAA simply does not do enough to protect employees' personal health data at the workplace.

Another issue is the fact that no federal agency is designated with overseeing or protecting employee health and fitness data. The issue could either be covered by the Food and Drug Administration (FDA) or the Federal Trade Commission (FTC), or both. Currently, there is somewhat of an overlap between both agencies regarding the protection of health and fitness data. However, Brown discusses how such an overlap can cause a number of problems: inconsistency, coordination challenges, and redundancy to name a few.[24] She then discusses both the FDA and FTC in detail. Because the FDA is most concerned with the efficacy of wearable products rather than privacy issues, Brown argues that the FTC is the best fit for federal oversight.[25] However, even the FTC has failed to properly address the issue. While they have noted that there is potential for employers to misuse health data and could become a concern, they have not taken any action to prevent future problems. Again, the protection of employee health data remains an issue that is lost in the shuffle, and without adequate recognition.

---

[23] 691 F.3d 1221; 2012 U.S. App.

[24] Brown, 12.

[25] Ibid, 13.

Another issue is on the side of the device manufacturers and app developers themselves. Currently, they face few legal restrictions when it comes to the collection and use of consumer health data. Brown elaborates on this issue:

> 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.[26]

Here, Brown discusses how consumers and their health data are not even protected by the manufacturer or developers of the apps they use. Not only may these parties share the data, they can sell it for profit without the users' consent or knowledge. Brown continues:

> 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.[27]

This is an important point, because the law has not even begun to regulate the activity of the companies that make the devices, such as Fitbit, or their respective mobile applications. The use of the devices at the workplace is a more recent, and somewhat unconventional way to use them. If the law is to change for employers and their use of health data, it will likely have to cover these parties as well.

It is clear that there is cause for concern in the potential misuse of employee health data. Employers currently enjoy a number of ethical loopholes that allow for countless discrimination and privacy issues in the future. While both HIPAA and ADAAA are good legal starting points, neither of them adequately address the issue. Though other laws have potential as well, none of them currently protect employee health and

---

[26] ibid., 14.

[27] ibid., 15.

fitness information explicitly. Additionally, without proper representation by a federal agency, the cause will continue to be minimized or ignored. In the digital age of today, it is imperative for the law to catch up to the boundless opportunities for employer misuse of health and fitness data.

Part IV: Potential Solutions and the Theoretical "Employee Health Data Collection Act"

There are a number of possible solutions that could remedy these legal loopholes. However, it is important to remember that the issue of protecting employee health data is a relatively recent phenomenon. The topic has yet to gain widespread attention, and extensive research has not been completed regarding solutions. In this section, I will analyze some of the proposed remedies discussed in prior works, as well as offer a suggestion of my own.

Some research has indeed been published on potential solutions to this legal issue. Brown offers two viable options in her review. One involves the FTC and their requiring health and fitness apps and devices to require privacy labels on their products. Currently, privacy policies are extremely difficult to locate on app and device websites. Moreover, the policies themselves are often pages long and perplexing to the average reader. For an example, Peppet cites a personal breathalyzer device and app that is connected to it. He notes that the breathalyzer came with a seventeen page manual and nowhere did it mention privacy. The app itself also failed to inform the user of the privacy policy, or if one even existed. He said that the privacy policy could only be found after after visited the app's website, and from there he scrolled through various pages and clicked on multiple links. After finally finding the link to the company's privacy policy,

he compared the process to “research.”[28] Once found, the policies often take a significant amount of time to read and comprehend. Unfortunately, this has become the norm for health devices and their related apps due to the lack of restriction. Brown suggests to incorporate a simple privacy labeling policy akin to nutrition facts printed on food labels. Essentially, all wearable devices would have a label on their packaging indicating a guarantee of privacy to the consumer.

Another solution would be to adjust the terms of HIPAA. Brown discusses this notion at length. HIPAA currently provides adequate privacy and protection of health data for “covered entities.” The issue is that employers are not clearly defined as covered entities in HIPAA. For covered entities, HIPAA provides specific security regulations regarding the confidentiality of electronic personal health data.[29] Moreover, it defines what proper use of data is, and protects against misuse.[30] For HIPAA’s “covered entities” to be redefined to include employers and their use of employee health data may be a step in the right direction, but it is still not enough.

Both pieces of Brown’s solution are certainly feasible options. As she discusses in her review, it would be relatively uncomplicated to implement a labeling policy, and it could be adopted in a short period of time. While mandatory privacy labels may be a good starting point, they don't specifically address the issue of protecting employee health data at the workplace. Additionally, if employees are given wearable devices through their workplace they will likely use them irregardless of a privacy label. In these

---

[28] Peppet.

[29] HIPAA Security Rule.

[30] HIPAA Privacy Rule.

instances, employees cannot be compared to consumers as they are not comparing different products to make an educated purchase. In effect, these privacy labels could be essentially nullified in the workplace. Next, her suggestion to adjust the terms of HIPAA and to redefine its “covered entities” would likely be a more tangible and effective answer. However, due to the specific nature of the issue of employee health data protection, as well as its technological element, it is time for a more radical change.

Rather than merely adjusting the verbiage of HIPAA, further policies must be created to fully protect employee health data. A new, comprehensive policy could elucidate exactly what employee health data is, and how it may be collected and used by employers. Theoretically speaking, the policy may be called the “Employee Health Data Protection Act” (EHDPA). First, any participation in corporate wellness programs or use or wearables at the workplace must be entirely voluntary on behalf of the employee. The EHDPA would clearly state that it is the employee’s decision to partake in any programs, and that no pressure may be made on the employer’s behalf. Additionally, it would state that any employee who chooses not to participate will not be punished in any way, nor will they experience negative consequences. This would prevent future instances of cases similar to Seff v. Broward County. As discussed earlier, Mr. Seff was charged $20 per paycheck for choosing not to submit personal health information via biometric screenings. The EHDPA would clearly define such a punishment as illegal for employers.

Next, the EHDPA would take several steps to further protect employee health data. First, the policy would state that employee health data collected by wearables must be fully anonymized. This would help to prevent employers from making

inferences based on an individual's information collected from their wearable device. However, this is still not enough. Even if anonymous, it may still be easy for an employer to match an employee with their data, especially if the company is small.

To fully protect any misuse of health data, the EHDPA must state that employers do not have access to any specific data, even once it has been anonymized. This section would require a third party to handle all data confidentially. This may appear to be an extreme measure, but it is the only way to guarantee that employees are fully protected. As discussed earlier, most employers incorporate wearable devices to reduce annual insurance costs. Typically, employers present employee health data to insurance companies to prove that their company is in better health and at lower risk than others. The EHDPA would change the steps of this process. As discussed, Fitbit already uses a corporate version of its software called Fitbit Wellness to track and collect health data from members of a specific corporation. Instead of employers having direct access to results, a third party such as Fitbit Wellness would provide results directly to the employer's insurance company. Because not all wearable devices have a program akin to Fitbit Wellness, another third party such as a data collection agency would suffice. The EHDPA would allow the third party to provide the employer with overall fitness trends of their companies, such as general improvements or regressions. However, employers will have absolutely no access to individualized health data, even after it has been anonymized. This way, employers will still have the benefit of reduced insurance costs without employees compromising their personal health information.

Moreover, the EHDPA would ensure that all data is confidential and may not be sold by the third party organization. Once collected by the third party, whether it be Fitbit

Wellness or a data collection agency, it may only be shared with pertinent entities such as the employer's insurance agency. Under the EHDPA, employee health may not be sold under any circumstances. As discussed earlier, no current law prevents employers or third parties from selling employee health data for profit. This is a major loophole that would by eliminated by the EHDPA.

Lastly, the EHDPA would ameliorate the current lack of transparency between employers and employees regarding personal health data. This section would require all employees to read and sign a document of full disclosure before agreeing to participate in the program. The document would educate the employee with explicit details concerning their personal health data, and how and why it will be used. First, it will state the precise categories of data collected, such as heart rate, slee patterns, steps taken, or any other fields of information. Next, the document must state that all data will be fully anonymized, and name the third party who will collect it, as well as the insurance company that will have access to it. The document must also inform the employee that their data will remain absolutely confidential, and will not be sold for profit under any circumstances. Finally, the document must clarify why and how the employee's health data is being used. If the employer reduces their annual insurance costs by giving their employees wearable devices, this must be clearly stated in the document. Naturally, the document must be tailored for each company, as each scenario has its unique circumstances. With the introduction of such a document, employees will learn exactly what data is being collected, how it is handled, and what it will be used for. Most importantly, it will assure the employee that their health data is fully protected.

The EHDPA would essentially seal the multiple gaps in the law concerning employee health data. The act would be all-encompassing, and eliminate the gray areas that exist when employers gain access to employee health data. If implemented, it would be impossible for employers to make unethical employment decisions based on health data, or for them to misuse it in other ways. Clearly, because the EHDPA is a theoretical policy that I have suggested, it is an idyllic solution. In reality, even if just one element of it were mandated into actual law, such as the requirement of third party collection or anonymized data, it would be a huge step towards a permanent solution. Until the gray area is eliminated, employers will continue to be able to exploit employees through their ability to misuse their health data.

Part V: Conclusion

As discussed, employee health data remains a largely overlooked and unprotected issue in current law. With the alarming growth of the Internet of Things, privacy issues regarding data, misuse is almost certain to happen in many forms. However, the issue of employee health data is an especially sensitive one. Employer misuse of personal health information, often collected by Fitbits and similar products, is an issue that the law must soon address. Promotions, hiring decisions, and discrimination are all outcomes that employees remain vulnerable to when they share health data with employers. Most employees are unaware of the degree of their vulnerability. Using a Fitbit through one's employer may seem like a harmless arrangement, but the law currently does not protect what an employer may do with it

and how they can use it. Unfortunately, it may take an extreme scenario that gains public attention for the law to adapt an adequate solution.

As discussed, the adjustment of HIPAA may be a good starting point, it is not enough to suffice as a complete solution. While my proposed EHDPA is again purely theoretical, it would entirely eliminate the potential for employers to misuse employee health data. The adoption of a policy similar to the EHDPA would essentially overhaul the existing system that allows for the numerous unethical practices discussed in this essay. Until this is reached, employees will remain vulnerable to the misuse of their personal health data in a growing number of ways.

Works Cited

45 C.F.R § 160.103. LexisNexis Code of Federal Regulations.

Ajunwa, Ifeoma, Kate Crawford, and Joel S. Ford. “SYMPOSIUM ARTICLE: CONTEMPORARY CHALLENGES IN INFORMED CONSENT: Health and Big Data: An Ethical Framework for Health Information Collection by Corporate Wellness Programs.”*, 44 American Society of Law, Medicine, and Ethics Journal of Law, Medicine, and Ethics 474.* (Fall, 2016): 5838 words. LexisNexis Academic. Accessed 9 Mar. 2017.

Brown, Elizabeth A. “The Fitbit Fault Line: Two Proposals to Protect Health and Fitness Data at Work.” *16 Yale Journal of Health Policy, Law, and Ethics 1.* (Winter 2016): 22865 words. LexisNexis Academic. Accessed 7 Mar. 2017.

BP Human Resources. “Shape Your Life: 2016 BP Wellness Program.” *BP Global,* 2016. http://hr.bpglobal.com/LifeBenefits/Assets/Documents/uvw/2016_BP_wellness_program_guide_online_FINAL.aspx. Accessed 2 March 2017.

Chen, Caroline, and Sharon Pettypiece. “Target to Offer Fitbits to 335,000 Employees.” *Bloomberg,* 15 Sep. 2015. https://www.bloomberg.com/news/articles/2015-09-15/target-to-offer-health-tracking-fitbits-to-335-000-employees

Fitbit, as quoted in Businesswire. “Fitbit Reports $574M Q416 and $2.17B FY16 Revenue, Sells 6.5M devices in Q416 and 22.3M devices in FY16.” *Business Wire,* 22 Feb. 2017. http://www.businesswire.com/news/home/20170222006497/en/Fitbit-Reports-574M-Q416-2.17B-FY16-Revenue/?feedref=JjAwJuNHiystnCoBq_hl-Q-tiwWZwkcswR1UZtV7eGe24xL9TZOyQUMS3J72mJlQ7fxFuNFTHSunhvli30RlBNXya2izy9YOgHlBiZQk2LOzmn6JePCpHPCiYGaEx4DL1Rq8pNwkf3AarimpDzQGuQ==

Fitbit. "Number of Active Users of Fitbit from 2012 to 2015 (in Millions)." Statista - The Statistics Portal, Statista, www.statista.com/statistics/472600/fitbit-active-users/, Accessed 5 Mar. 2017.

Fort, Timothy L, Anjanette H. Raymond, and Scott J. Shackelford. “The Angel on Your Shoulder: Prompting Employees to Do the Right Thing Through the Use of Wearables.” *14 Northwestern Journal of Technology and Intellectual Property 139.* (2016): 10549 words. LexisNexis Academic. Accessed 9 Mar. 2017.

HIPAA Privacy Rule, 45 C.F.R. parts 160, 164(A), 164(E) (2003).

HIPAA Security Rule, 45 C.F.R. parts 160, 164(A), 164(C) (2003).

Levy, Douglas. “Wearing your Private Data on Your Sleeve.” *Michigan Lawyers Weekly,* 12 Feb. 2016: 876 words. LexisNexis Academic. Accessed 8 Mar. 2017.

Liu, Josephine. “FTC Working on Privacy ‘Nutrition Label’; Industry Focusing on Icons,” *Inside Privacy.* Oct. 25, 2012. http://www.insideprivacy.com/united-states/federal-tradecommission/ftc-working-on-privacy-nutrition-label-industry-focusing-on-icons. Accessed 6 April 2017.

Magnuson-Moss Warranty-Federal Trade Commission Improvement Act, Pub. L. No. 93-637, 88 Stat. 2183 (1975) (codified as amended at 15 U.S.C § 2301-12 (2012)).

Peppet, Scott R. “Article: Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent.” *93 Texas Law Review 85.* (November 2014): 41384 words. LexisNexis Academic. Accessed 9 Mar. 2017.

Satariano, Adam. “Wear This Device So the Boss Knows You’re Losing Weight.” *Bloomberg,* 21 Aug. 2014. https://www.bloomberg.com/news/articles/2014-08-21/wear-this-device-so-the-boss-knows-you-re-losing-weight. Accessed 5 Mar. 2017.

“SEFF v. BROWARD COUNTY:” 691 F.3d 1221; 2012 U.S. App. LEXIS 17501; 26 Am. Disabilities Cas. (BNA) 1153; 23 Fla. L. Weekly Fed. C 1432; 15 Accom. Disabilities Dec. (CCH) P15-092. LexisNexis Academic. Web. Date Accessed: 2017/03/11.

Seitz, Patrick. “Target Offers Fitbit Trackers To All U.S. Staff; Fitbit Stock Pole-Vaults 12%; Wearables are trendy, but will workers' health, medical costs improve?." *Investor's Business Daily,* 17 Sep, 2015: 427 words. LexisNexis Academic. Accessed 4 Mar. 2017.