Navigating Workplace Wellness Programs in the Age of Technology and Big Data

Hannah-Kaye Fleming
Sandra Day O'Connor College of Law, Arizona State, J.D. Candidate (2021)
http://doi.org/10.38126/JSPG170104
Corresponding author: hkflemin@asu.edu
Keywords: workplace wellness programs, privacy, data, technologies, HIPAA, employer, employee

Executive Summary: Workplace wellness programs come in a myriad of forms, each with the goal of improving employee health and productivity while reducing healthcare costs. In the age of big data, wearable devices are ubiquitously incorporated into workplace wellness programs. Wearable devices in wellness programs can be beneficial for employers, employees, and health insurers alike. Nevertheless, there is an increasingly complex risk landscape associated with wearable devices in wellness programs, raising profound legal and ethical concerns related to privacy, security, information abuse, and employee autonomy. This paper will discuss the benefits and challenges of wearable devices in workplace wellness programs. Part I will introduce the benefits of workplace wellness programs. Part II will discuss the incorporation of wearable technologies in workplace wellness programs. Part III will analyze the legal and ethical challenges associated with the use of wearable technologies in wellness programs. Finally, Part IV will propose soft law, or best practices, as the most efficacious governance mechanism for employers and employees to secure benefits and balance concerns associated with the use of wearable devices in workplace wellness programs.

I. Introduction to workplace wellness programs

Workplace wellness programs are predicted to be a $12 billion industry by 2020 (Turk 2016). Wellness programs come in countless forms but share a common goal: improving employee health and productivity while reducing healthcare costs. Employers around the country utilize wellness programs to motivate employees to adopt and maintain behaviors such as weight management, healthy eating, and tobacco cessation. Wellness programs may also offer employees disease management counseling, preventative screenings, and encouragement and support. Employees participating in a wellness program will generally receive a health risk assessment ("HRA") offered by their employer to assess their potential health risks and set wellness goals. HRAs help the employee, the employer, and the healthcare provider create a custom health and wellness plan tailored to the specific employee's needs.

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") first authorized workplace wellness programs (U.S. Department of Health & Human Services 2019). HIPAA created an exception to the general rule prohibiting group health plans from varying premiums or determining eligibility based on an individual's health status. Under HIPAA, employees participating in qualified workplace wellness programs may be eligible for cost-sharing reductions or premium discounts of up to 20% (Schilling 2011). Wellness programs continue to receive governmental support through the Affordable Care Act's ("ACA") wellness program requirements. Under the ACA, employees who participate in their employer's wellness program and meet specific biometric goals may be eligible for health insurance premium discounts of up to 30% (Jones 2019).

Workplace wellness programs have proliferated since the passage of the ACA. In 2019, over 84% of employers offering health insurance provided

wellness programs (Keith 2019). Wellness programs may provide a win-win benefit to both the employer and employee when employees improve their health and well-being—offsetting rising healthcare costs. Additionally, employers' benefit from lower health-related employee absenteeism and turnover, along with increased worker productivity and job satisfaction.

Nevertheless, the Equal Employment Opportunity Commission's ("EEOC") current rules governing workplace wellness programs remain unclear (Smith 2017). Critics raise valid concerns that wellness programs require disclosure of sensitive information and penalize and discriminate against employees in poorer health. Recent research also suggests wellness programs may not provide the benefits they promise. The Illinois Workplace Wellness Study ("IWWS")—a randomized control trial of 5,000 employees conducted from October 2016 to April 2017—showed varied results (Jones 2019). Although participants engaged in healthier behaviors like joining a gym, there was no significant impact on other factors typically associated with program success like health-related employee absenteeism, job performance, healthcare outcomes, or healthcare spending (Jones 2019).

Despite the IWWS's varying results, the use of technology and big data may revitalize wellness programs. Employers are increasingly relying on wearable devices ("wearables") to simplify their wellness programs and provide more accurate and tangible healthcare data. The following section discusses the proliferation of wearable devices in workplace wellness programs.

II. Benefits of wearable devices in workplace wellness programs

Wearable devices are often worn in the form of a bracelet or watch that employs kinetic, electrochemical, and biological sensors to monitor a person's specific movements, interactions, and exposures (Marchant 2019). These devices, such as Fitbits, are among the fastest growing subsets of the Internet of Things (IoT). The IoT consists of devices equipped with nanosensors, microchips, and wireless communication capabilities, allowing for the transfer of large quantities of data across multiple networks (Thierer 2015). Consumers have rapidly adopted the useful connectivity of wearable devices: the global wearable device market is expected to increase at a compound annual rate of 17.66% between 2019 and 2024 (Wood 2019).

Employers are increasingly integrating wearable fitness devices into their wellness programs to improve employee participation and engagement. Currently, 40 to 50% of wellness programs incorporate wearable devices (Haggin 2016). Gartner, a research and advisory firm, predicts that 90% of workplace wellness programs will include wearable devices by 2021 (Pettey 2018). Another recent study by ABI Research estimates that 44 million wearable devices will be incorporated into wellness programs by 2021 (Sielinksi 2018). The use of wearable fitness devices in conjunction with wellness programs may provide employers and employees substantial benefits.

Wearable fitness devices are built to incentivize exercise and other healthy behaviors. Employees may be more attuned to early disease indicators or adverse health exposures by monitoring their progress through wearable fitness devices (Marchant 2019). Employees can also track their mood, health indicators, steps, sleep, heart rate, and physical activity, better equipping them to reach their health goals. Research has shown that self-tracking devices can facilitate healthy behaviors, such as weight loss, and better help users monitor chronic illnesses (Schutte 2014).

Healthier living leads to happier employees and potentially increased workplace productivity. A study by Goldsmiths at the University of London held that wearable technology has the potential to boost employee job satisfaction and productivity by up to 8.5% (Schutte 2014). Additionally, the use of wearables may result in significant healthcare savings for employers and employees. For example, Apprior, an information technology consulting firm, reduced its insurance costs by $280,000 by sharing data collected from employees' wearable devices with its health insurer (Gohring 2014). The comprehensive volume of personal health data collected through wearables also benefits health insurers by allowing them to better assess policyholders' risks and future costs (Olson 2014).

Wearable devices are beneficial to all parties and provide an innovative and efficient way for

workplace wellness programs to gather data about an employee's physiological and physical characteristics. However, the use of wearable devices in wellness programs presents additional legal and ethical challenges in the workplace.

III. Legal and ethical challenges surrounding the use of wearable devices in workplace wellness programs

Challenges associated with the proliferation of wearables in wellness programs include inadequate privacy and security regulations, the possibility of information abuse, discrimination, and reduced employee autonomy.

i. Inadequate privacy regulations

As wearable devices in workplace wellness programs become ubiquitous, concerns surrounding data privacy escalate. Unlike the European Union— which adopted comprehensive privacy legislation regulating how consumer data is processed and transferred— the United States lacks a comprehensive privacy legislation (International Trade Administration 2020). Consumer data is inadequately protected by current piecemeal privacy laws in the United States (O'Connor 2018). Data privacy protections in the United States amount to a legal jigsaw puzzle. Protection may vary based on who is collecting the data, the type of data collected, and data usage. In wellness programs, data may be shared simultaneously between the employer, insurer, wellness program vendor, and/or the device manufacturer. Thus, it is often unclear which privacy regulations apply to data collected and shared through workplace wellness programs.

Many employees participating in workplace wellness programs mistakenly believe that the HIPAA Privacy Rule protects the health data collected from their Fitbit or Apple Watch. Under HIPAA, covered entities, including healthcare providers, healthcare clearinghouses, health insurance plans, and their business associates, are required to protect "personal health information" (PHI) (45 C.F.R. § 160.103). PHI is defined as health information, including demographic information, that "identifies the individual or...[gives] a reasonable basis to believe that information can be used to identify the individual" (45 C.F.R. § 160.103). De-identified data collected from wearable devices in workplace wellness programs does not constitute PHI and therefore is not protected under HIPAA (45 C.F.R. § 160.103).

Additionally, HIPAA protects data collected in conjunction with a group health insurance plan, but not data collected through a private wellness vendor. Employers often contract with corporate wellness vendors, like Sonicboom, to independently structure their workplace wellness programs. Because neither the employer nor the vendor would be considered a covered entity, the collected data lacks HIPAA protection.

Further, HIPAA offers no private right of action or enforcement (45 C.F.R. § 160.103). HIPAA vests exclusive enforcement power in the Secretary of the Department of Health and Human Services and State Attorney Generals (U.S. Department of Health & Human Services 2017). Therefore, employees cannot legally enforce their right to privacy under HIPAA, even if HIPAA protects the data collected from their wearable device.

Wearable devices also lack U.S. Food and Drug Administration ("FDA") oversight. The FDA oversees the regulation of medical "devices" through the Food, Drug, and Cosmetic Act of 1938 (21 U.S.C. § 321). "Devices" include instruments "intended for use in the diagnosis of a disease or other conditions" (21 U.S.C. § 321(h)(2)). However, FDA guidance suggests it will not "vigorously regulate devices" that generally encourage healthy behaviors and are not harmful or medically invasive (Center for Devices and Radiologist Health 2019).

Other existing federal privacy frameworks also inadequately protect employee data collected from wearables in wellness programs. For example, the Electronic Communications Privacy Act of 1986 ("ECPA"), which prohibits intentional interception and disclosure of electronic communications and data, explicitly exempts "tracking devices which permit the tracking of movement of a person or object" (Langley 2015). Thus, ECPA protections do not apply to wearable technologies. Additionally, employees forfeit ECPA protection by consenting to data collection in a workplace wellness program.

This lack of comprehensive federal privacy protections has incentivized state action. The California Consumer Privacy Act ("CCPA") of 2018

creates new statutory privacy rights to better protect California citizens' personal information (Hirsch 2019). The CCPA went into effect on January 1, 2020 and gives California consumers the right to access their data and request that a company delete their data and also prevents the sale of their data to third-parties. However, the CCPA does not protect personal information that is anonymized. Because data collected from wearable devices in wellness programs is generally de-identified, employees' personal data is likely unprotected. This loophole creates a critical issue because of the ability to re-identify individuals' personal data. Re-identification is highly probable when anonymized data is analyzed using outside sources of non-anonymous information, such as mobile phone locations or credit card purchases (Wakabayashi 2019).

Although the CCPA has motivated other states like Nevada and New York to propose similar laws, there are currently no proposals for comprehensive federal protection. Current data privacy regulations inadequately protect employee data collected from wearables in wellness programs.

ii. Inadequate data security protections

Present-day security law does not adequately protect data collected from wearables in wellness programs. Many wearable devices have a higher risk of being hacked because they lack built-in security measures, and their small forms make it difficult to integrate the necessary processing power to maintain these measures. Further, the simultaneous sharing of data in wellness programs presents additional opportunities for hackers. Data security in the United States is typically regulated by one of two mechanisms: The Federal Trade Commission Act ("FTC Act") or state data breach notification laws. Additionally, the HIPAA Security Rule applies to a subset of entities processing electronic personal health information ("ePHI").

Under the FTC Act, the Federal Trade Commission ("FTC") has the authority to bring legal action against companies for security breaches (15 U.S.C. § 45(a)(1)). The FTC has prosecuted numerous companies for failing to maintain adequate cybersecurity measures that protect consumer data from hackers. However, the FTC does not require companies meet specific security standards. Instead, the FTC provides ex post facto solutions once data security is compromised and a consumer or employee suffers an injury (Spinelli 2014). The FTC's lack of prevention power leaves users of wearable devices vulnerable and at risk of unauthorized or inappropriate use of their personal information by others.

State data breach laws may also fall short in providing adequate security measures for wearable devices in workplace wellness programs. All 50 states have some form of a data breach notification law, requiring disclosure if and when an individual's personal data is compromised (NCSL 2018). Similar to FTC enforcement, these laws fail to provide sufficient security measures and provide only ex post facto protections. Also, under most state laws, personal information is generally limited to information like an individual's first and last name, driver's license number, credit card number, and social security number. A breach of anonymized personal health data likely does not trigger most state data breach laws.

Users of wearable devices often mistakenly believe that the HIPAA Security Rule ("Security Rule") protects their health data (U.S. Department of Health & Human Services 2003). However, like the HIPAA Privacy Rule, the Security Rule does not provide adequate protection for the reasons mentioned above. If employee data is collected in the aggregate and de-identified, the data may lose all HIPAA security protections. However, many non-covered entities have adopted the HIPAA Security Rule as the company's security standard. For example, Fitbit became HIPAA compliant after cybercriminals hacked users' devices in 2015. However, voluntary compliance by non-covered entities is not legally enforceable.

Ensuring the security of wearable devices is critical in the age of technology and big data. Employees cannot be sure how data collected from their wearables will be used, with whom it will be shared, and how it will be protected. The lack of adequate privacy and security protections puts employees at risk of information abuse and discrimination. The following two sections discuss the ethical implications of wearable devices in workplace wellness programs.

iii. The potential for information abuse and discrimination

Inadequate privacy and security laws regulating wearable devices in wellness programs present additional concerns. Without establishing proper mechanisms, employees may be at risk of discrimination in the workplace. Employers could analyze the data from wearable devices to help inform their promotion and firing decisions (Brown 2017). Employers may favor employees who are meeting their health goals over employees whose biometric data is more concerning. Thus, employers may associate employees in worse physical health with being less productive and more costly (Brown 2017). For example, an employer looking to promote an employee to an executive-level position may believe an active employee in good health is more motivated, and thus better qualified for the job. Hiring based on individual health status rather than merit is arguably unfair. Although employees may be better protected from information abuse and discrimination when the data is de-identified, anonymous data is not inviolable. An MIT study found that continuing advancements in technology and computer science make re-identification of anonymous data easier (Matheson 2018). The study also confirmed that the sensors in wearable devices are especially vulnerable to attack.

Furthermore, employees may not realize the risk of their personal data being sold to third parties. Third parties may use employees' health data to assess their creditworthiness, affect their health insurance premiums, and design personally targeted ads (Britton 2015). Additionally, the data collected from a wearable device may be used to create false assumptions. For example, poor sleeping patterns brought on by a bad mattress may incorrectly be associated with an employee having depression, a mental illness, or a drug or alcohol dependency (Piwek 2016).

Moreover, workplace wellness programs must comply with the Americans with Disabilities Act of 1990 ("ADA") and the Genetic Information Nondiscrimination Act of 2008 ("GINA") because wellness programs allow employers to collect sensitive health information from participating employees (42 U.S.C §12101). The ADA prohibits employers from requiring medical examinations and making other disability inquires unless necessary and related to the employee's job position. Similarly, GINA bars employers from requiring family medical history or genetic information, including results of genetic tests or services, as a precondition of employment. But, to the benefit of employers, both the ADA and GINA contain voluntary exceptions. Workplace wellness programs are compliant with the ADA and GINA when they are voluntary and consensual. However, both statutes fail to define "voluntary," raising ethical concerns regarding employee autonomy and coercion. When participation is tied to financial incentives or rewards, the decision to participate may place employees in a conundrum. Many employees are likely opposed to the idea of being monitored continuously through their employer's workplace wellness program. Yet, a significant incentive or reward may make refusal difficult. Critics like the American Association of Retired Persons (AARP) argue that high financial incentives may undermine employees' real choice in participation, diminishing employee autonomy in the workplace (Health Affairs 2020).

iv. Ethical considerations regarding employee autonomy

With the growth of the IoT, employee surveillance is becoming omnipresent. As wearable devices become ubiquitous in wellness programs, employers can closely monitor employee behaviors outside of work. The use of wearable devices outside of work may result in constant monitoring, blurring the line between an employee's professional and personal life. Employee advocates argue that the perception of being constantly monitored by an employer creates additional pressure and stress which may decrease overall workplace morale (Wolfe 2018). Employees may feel a sense of reduced autonomy knowing their employer has knowledge and control over their personal health data. Arguably, few employees feel comfortable with an employer monitoring their health behaviors and having access to their biometric outcomes (Reed 2018).

Additionally, the employer-employee relationship may reduce employee willingness to refuse participation when there are obvious workplace benefits for the employer. Employees may fear they will experience shame or stigma in the workplace if they refuse to participate. Additionally, consenting to the use of wearable devices in wellness programs

creates additional complexities. Informed consent documents often contain immense blocks of legal jargon that the average employee cannot comprehend. Being unaware of or misunderstanding how data is utilized or where it is going further minimizes employee autonomy.

Current EEOC regulations leave employers uncertain about when a wellness program is voluntary. In AARP v. United States EEOC, the AARP argued against the EEOC's adoption of the ACA's 30% incentive for employee participation in workplace wellness programs. The AARP argued that a 30% discount on healthcare coverage was too high, undermining the requirement that wellness programs be voluntary (Keith 2019). The Court ordered the wellness incentive rule vacated if not revised by January 1, 2019. On June 11, 2020, the EEOC agreed to proceed with a new proposed rule prohibiting most types of wellness programs from incorporating incentives to engage employees. For a workplace wellness program to be considered "voluntary," wellness programs can only offer de minimis incentives (Health Affairs 2020). However, it is unclear what constitutes a de minimis incentive. In the absence of clear guidelines for appropriate incentive levels, employers should consider ethical issues regarding employee autonomy.

Requiring adequate privacy and security measures for wearable devices in workplace wellness programs will do more than protect employees from potential information abuse and discrimination. Data privacy and security are integral to employee autonomy and beneficial for society. The following section recommends the use of soft law—recommendations or best practices—to avoid the legal and ethical challenges associated with the proliferation of wearable devices in workplace wellness programs. In the absence of comprehensive federal and state regulations, applying soft law is critical for employers and employees to reap the benefits of workplace wellness programs.

IV. The use of soft law to navigate legal and ethical challenges

Employers and employees are each subject to high risk and liability because of the lack of federal and state law governing the use of wearable devices in workplace wellness programs. Strict legal solutions may inadequately match the rapid advances in technology. Scholars refer to this as the pacing problem, which is the inability for top-down regulations to match the fast speed at which technology, consumer demands, and business practices change (Thierer 2018). Technologies, like wearable fitness devices, will continue to advance in the workplace. For example, tattoos, implants, and even ingestible devices are forming the next generation of wearable technology (Thierer 2015). To match the pace of technological advancements and avoid the legal pitfalls associated with the use of wearable devices in workplace wellness programs, employers should apply soft law.

The following best practices are based on current understanding of the IoT, workplace wellness programs, and wearable technologies. Following these guidelines will allow employers and employees to better navigate workplace wellness programs in the age of technology and big data.

i. Voluntary participation

Voluntary employee participation is essential to the success of wearable devices in workplace wellness programs. Workplaces that do not give employees free choice to participate are likely to reduce employee morale and negate the potential benefits of wellness programs. Additionally, employees should have a voice and be involved in the creation and implementation of the wellness program. Employers should also actively ensure that non-participating employees are not penalized.

ii. Data transparency

The proliferation of wearable technologies in workplace wellness programs allows employers and other stakeholders to collect substantial amounts of employee data. To cultivate employee cooperation and trust in the program, employees must be well-informed. However, current business privacy disclosures fail to inform employees adequately. First, employers should fully disclose to employees how the wearable technologies operate, what data is collected, and who has access to the information. The informed consent process should not be filled with legal jargon. This will ensure that employees make fully informed decisions regarding the privacy and security risks associated with wearable technologies. Second, employers should not give third parties access to employee data without obtaining earlier informed consent from their

employees. Additionally, employers should contractually hold third parties with access to employee data to the employer's privacy and security standards. Finally, employees should have access to their data, any conclusions drawn from the analysis thereof, and the ability to have data erased. Open transparency will heighten employee trust in the employer, wearable device, and wellness program.

iii. Secure data collection and control

When vast amounts of data are collected, privacy and security are of primary concern. Data privacy and security have been dubbed "the Wild West" absent comprehensive enforceable regulations. Employers should proactively adopt adequate privacy and security measures and communicate any changes to company standards with all employees. Proactive measures include performing ongoing security notices and software updates, minimizing the life span of unnecessary data, and ensuring all data is collected in the aggregate, encrypted, and de-identified. Employers should also create a process to routinely identify internal and external threats to data privacy and security. Although not legally binding for all employers, HIPAA's Privacy and Security Rule, the General Data Protection Regulation (GDPR), and the CCPA may provide additional guidance for employers to model.

iv. Credible technologies

Often, data collected from wearable devices is inaccurate or inconsistent. Users may be unaware of or unable to correct transmission errors. Wearable device consumers have filed a multitude of complaints and lawsuits alleging that their device inaccurately calculated data. Before implementing a wearable device into a workplace wellness program, employers should research the device's reliability. Inaccurate and inconsistent data collection will allow neither the employer nor the employee to benefit from the device. Incorrect data may also be detrimental to employee health and safety, contributing to worse health outcomes.

Although legally unenforceable, employers can benefit by applying soft law as a mechanism to regulate the use of wearable devices in workplace wellness programs. Employers should incorporate best practices into their wellness programs because of market concerns regarding privacy and security (Holden 2019). Moreover, the use of soft law can shape norms around workplace wellness programs and inform future laws without suffocating technological advancements and innovation. Proactive solutions will enable employers to safely navigate the legal and ethical conundrums associated with the use of wearables in wellness programs, raising the chance of program success (Marchant 2019).

V. Conclusion

Wearable devices have become permanent fixtures in workplace wellness programs. For employers and employees, the incorporation of wearables in wellness programs may have tremendous benefits. However, the proliferation of wearables in wellness programs creates additional legal and ethical challenges. Current piecemeal federal and state legislation in the United States inadequately protects data collected from wearable devices, putting employees and employers at risk. Inadequate privacy and security standards may serve as a vehicle for information abuse, discrimination, and may reduce overall employee autonomy and morale. To reap the potential benefits of wearable devices in wellness programs, employers should apply soft law, in the form of adopting best practices, to better safeguard employees' health data. Ensuring wellness programs are employee-centric and focused on privacy and security will provide better outcomes for all stakeholders.

References

Britton, Katherine. 2015. "IoT Big Data: Consumer Wearables, Data Privacy and Security," *American Bar Association*. December 2015. https://www.americanbar.org/groups/intellectual_property_law/publications/landslide/2015-16/november-december/IoT-Big-Data-Consumer-Wearables-Data-Privacy-Security/.

Brown, Elizabeth. 2017. "Workplace Wellness: Social Injustice," *N.Y.U Journal of Legislation & Public Policy*. April 20, 2017. https://nyujlpp.org/wp-content/uploads/2017/04/Brown-Workplace-Wellness-Social-Injustice-20nyujlpp191.pdf.

Center for Devices and Radiologist Health. 2019. "General Wellness: Policy for Low Risk Devices," *U.S. Food & Drug Administration*. September 2019. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices.

Gohring, Nancy. 2014. "Saving on Insurance with Fitbit," *Preventure.* July 16, 2014. https://preventure.com/saving-on-insurance-with-fitbit/.

Haggin, Patience. 2016. "As Wearables in Workplace Spread, So Do Legal Concerns," *Wall Street Journal.* March 13, 2016. https://www.wsj.com/articles/as-wearables-in-workplace-spread-so-do-legal-concerns-1457921550.

Health Affairs Blog. 2020. "EEOC will Advance New Wellness Regulations," *Health Affairs*.

Hirsch, Reece et. al. 2019. "INSIGHT: CCPA Amendments to Watch as Effective Date Draws Closer," *Bloomberg Law*. October 2, 2019. https://news.bloomberglaw.com/privacy-and-data-security/insight-ccpa-amendments-to-watch-as-effective-date-draws-closer.

Holden, Jenner. 2019. "Data Security and Privacy," *Remarks at the Sandra Day O'Connor College of Law.* October 23, 2019.

International Trade Administration. 2020. "European Union – Data Privacy and Protection," *ITA*. June 2020. https://www.trade.gov/european-union-data-privacy-and-protection.

Jones, Damon, et al. 2019. "What Do Workplace Wellness Programs Do? Evidence from Illinois Workplace Wellness Study," *Natural Bureau of Economic Research.* January 2019. http://www.nber.org/papers/w24229.

June 17, 2020. https://www.healthaffairs.org/do/10.1377/hblog20200617.824130/full/.

Keith, Katie. 2019. "HHS Proposes New Wellness Demonstration Projects," *Health Affairs.* October 1, 2019. https://www.healthaffairs.org/do/10.1377/hblog20191001.231439/full/.

Langley, Matthew. 2015. "Hide your Health: Addressing the New Privacy Problem of Consumer Wearables," 103 Geo L.J. 1641, 1652 (2015).

Marchant, Gary. 2019. "What are Best Practices for Ethical Use of Nanosensors for Worker Surveillance?" AMA J. Ethics 356 https://journalofethics.ama-assn.org/article/what-are-best-practices-ethical-use-nanosensors-worker-surveillance/2019-04.

Matheson, Rob. 2018. "The Privacy Risks of Compiling Mobility Data," *MIT News Office.* December 7, 2018. http://news.mit.edu/2018/privacy-risks-mobility-data-1207.

NCSL. 2018. "Security Breach Notification Laws," *National Conference of State Legislatures*. September 29, 2018. http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

O'Connor, Nuala. 2018. "Reforming the U.S. Approach to Data Protection and Privacy," *Council on Foreign Relations.* January 30, 2018. https://www.cfr.org/report/reforming-us-approach-data-protection.

Olson, Parmy. 2014. "Wearable Tech is Plugging Into Health Insurance," *Forbes.* June 19, 2014. https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/#26e2266718bd.

Pettey, Christy. 2018. "Data From Wearables is Gaining Acceptance in Healthcare Communities," *Gartner.* March 8, 2018. https://www.gartner.com/smarterwithgartner/wearables-hold-the-key-to-connected-health-monitoring/.

Piwek, Lukasz et. al. 2016. "The Rise of Consumer Health Wearables: Promises and Barriers," *PLoS medicine* vol. 13, 2 e1001953. 2 Feb. 2016, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4737495/.

Reed, Robert. 2018. "Workplace Monitoring Gets Personal, and Employees Fear it's too Close for Comfort. They're Right," *Chicago Tribune*. March 2, 2018. https://www.chicagotribune.com/business/ct-biz-amazon-workplace-privacy-dilemma-robert-reed-0304-story.html.

Schilling, Brian. 2011. "What do HIPAA, ADA, and GINA Say About Wellness Programs and Incentives," *The Commonwealth Fund*. September 19, 2011. https://www.commonwealthfund.org/publications/newsletter-article/what-do-hipaa-ada-and-gina-say-about-wellness-programs-and.

Schutte, Shané. 2014. "Wearable Technologies can Boost Employee Productivity," *Real Business*. May 1, 2014. https://realbusiness.co.uk/wearable-technologies-can-boost-employee-productivity/.

Sielinksi, Dave. 2018. "Wearable Technology May Boost Wellness but Be Careful," *SHRM.* June 5, 2018. https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/wearable-technology-boost-wellness-be-careful.aspx.

Smith, Allen. 2017. "EEOC Ordered to Reconsider Wellness Rules," *SHRM*. August 24, 2019. https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/aarp-eeoc-wellness-regulations.aspx.

Spinelli, Cooper. 2014. "Far from Fair, Father from Efficient: The FTC and the Hyper-Formalization of Informal Rulemaking," Legislation and Policy Brief 6, n.1 Article 3(2014), http://digitalcommons.wcl.american.edu/lpb/vol6/iss1/3.

The Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 321 (1964).

The Federal Food, Drug, and Cosmetic Act, 21 U.S.C. § 321(h)(2) (1964).

The Federal Trade Commission Act, 15 U.S.C. § 45(a)(1) (1914).

The Health Insurance Portability and Accountability, 45 C.F.R. § 160.103 (1996).

Thierer, Adam. 2015. "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation," 21 Rich. J.L. & Tech. http://jolt.richmond.edu/v21i2/article6.pdf.

Thierer, Adam. 2018. "The Pacing Problem and the Future of Technology Regulation," *Mercatus Center*. August 8, 2018. https://www.mercatus.org/bridge/commentary/pacing-problem-and-future-technology-regulation.

Turk, Sarah. 2016. "All is well: The Industry Will Exhibit Robust Growth as Business Rapidly Adopt Wellness Programs," *IBIS World*. February 2016. http://static.politico.com/3e/68/b29a1ff04e7d8bc7c8231352ffc5/ibis-study-on-corporate-wellness-programs.pdf.

U.S. Department of Health & Human Services. 2003. "Health Insurance Reform: Security Standards," *Federal Register*. February 20, 2003. https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf?language=es.

U.S. Department of Health & Human Services. 2017. "State Attorneys General," *HHS.* December 21, 2017. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/state-attorneys-general/index.html.

U.S. Department of Health & Human Services. 2019. "Summary of the HIPAA Privacy Rule," *HHS.* October 30, 2019. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html.

Wakabayashi, Daisuke. 2019. "Google and the University of Chicago Are Sued Over Data Sharing," *New York Times*. June 26, 2019. https://www.nytimes.com/2019/06/26/technology/google-university-chicago-data-sharing-lawsuit.html.

Wolfe, Julia. 2018. "Coerced into Health: Workplace Wellness Programs and Their Threat to Genetic Privacy," 103 Minn. L. Rev. 1089 (2018). https://scholarship.law.umn.edu/cgi/viewcontent.cgi?article=1069&context=mlr.

Wood, Laura. 2019. "Worldwide Wearable Technology Market (2019-2024) Analysis by Product & Geography – North America to Hold Major Share," *PR Newswire*. June 21, 2019. https://www.prnewswire.com/news-releases/worldwide-wearable-technology-market-2019-2024-analysis-by-product--geography---north-america-to-hold-major-share-300872692.html.

Hannah-Kaye Fleming: is a third-year law student at the Sandra Day O'Connor College of Law. She will graduate in May 2021 with her J.D. and a certificate in Health Law. Hannah graduated Summa Cum Laude from Auburn University with a degree in Healthcare Administration.

Acknowledgements
The author would like to thank both Gary Marchant and Guy Cardineau for their insightful feedback.