

2-28-2019

Notice and Consent: A Healthy Balance Between Privacy and Innovation for Wearables

Erika J. Nash

Follow this and additional works at: <https://digitalcommons.law.byu.edu/jpl>



Part of the [Health Law and Policy Commons](#)

Recommended Citation

Erika J. Nash, *Notice and Consent: A Healthy Balance Between Privacy and Innovation for Wearables*, 33 BYU J. Pub. L. 197 (2019).
Available at: <https://digitalcommons.law.byu.edu/jpl/vol33/iss1/10>

This Comment is brought to you for free and open access by BYU Law Digital Commons. It has been accepted for inclusion in Brigham Young University Journal of Public Law by an authorized editor of BYU Law Digital Commons. For more information, please contact hunterlawlibrary@byu.edu.

Notice and Consent: A Healthy Balance Between Privacy and Innovation for Wearables

I. INTRODUCTION

In our culture of continuous technological advancement, society has never more effectively monitored and interpreted the daily actions of individual living. At the core of data monitoring advancements are wearable devices (“wearables”), which are often worn directly on the bodies of individuals and used to capture, aggregate, and analyze a wide range of personal health data. Such devices not only provide individuals greater insight into their daily actions, but also present an opportunity to share generated information with interested third-parties, including health care providers and insurance companies. Continued user adoption has positioned wearables not only to be an important consumer product, but also to command significant regulatory attention. While meaningful benefits likely accompany such widespread adoption, have the unavoidable costs of questionable device utility, data-breach threats, and discriminatory applications of generated data been fully considered?

This paper evaluates the societal impact of wearables and how America’s limited regulatory landscape is ill-equipped to effectively respond to various legal issues relating to broad generation and dissemination of personal health data.¹ Part II of this paper provides a foundational background that explains emerging wearable technology and outlines the accompanying benefits and drawbacks of the devices. Part III examines the current landscape of regulation designed to protect personal health data and explores the sufficiency of such as it relates to wearables. Part IV suggests that, rather than adopting comprehensive

1. Several articles similarly explore the current regulatory challenges associated with wearables, including Alexandra Troiano, Note, *Wearables and Personal Health Data: Putting a Premium on Your Privacy*, 82 BROOK. L. REV. 1715 (2017). Both the Troiano article and this paper consider the benefits and drawbacks of wearables along with the current regulatory landscape, and subsequently propose recommended solutions to the identified challenges. This paper, however, expands the scope of Troiano in at least three important ways: first, by highlighting the questionable device utility of wearables—a crucial element of the debate; second, by identifying and emphasizing that wearable data can potentially be used for discriminatory purposes—another relevant point for consideration; and, third, by proposing an alternative solution for how best to protect personal health data in the United States—that is, to implement limited regulation that provides users with clear notice and consent.

regulation like the General Data Protection Regulation (“GDPR”) of the European Union, the United States should pursue solutions that promote commercial innovation, which is essential to reducing the high costs of health care. More specifically, the government should consider implementing only limited regulation, modeled after certain provisions of the GDPR, that provides users with clear notice and consent regarding the privacy policies of associated data generating devices and applications. Part V concludes.

II. WEARABLE DEVICE TECHNOLOGY

Wearable technology refers to any electronic device with sensors, typically worn on the body, that is used to collect and deliver information about their surroundings—traditionally, health and fitness related activities.² Though most commonly worn on the wrist,³ wearables come in a variety of forms (e.g., watches, glasses, belts, shirts, shoes, jewelry, implants, etc.)⁴ and are often designed to remain on the body of a user at all times.⁵ As part of a larger category of products known as the “Internet of Things,”⁶ wearables are equipped with sensors that measure and analyze⁷ a range of activity—and many devices are capable of being accessed and controlled remotely across a network infrastructure.⁸

2. Sandra Chefitz, June Quah & Adnan Haque, *Stratifying Mortality Risk Using Physical Activity as Measured by Wearable Sensors*, 1 MUNICH RE 8, 1 (2018), https://www.munichre.com/site/marclife-mobile/get/documents_E-889788279/marclife/asset.marclife/Documents/Publications/Stratifying_Risk_Using_Wearable_Data.pdf.

3. Matthew R. Langley, Note, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 GEO. L.J. 1641, 1642 (2015).

4. *Id.* at 1643; see also Troiano, *supra* note 1, at 1716.

5. Langley, *supra* note 3, at 1643–44.

6. A “thing” is any object with embedded electronics that can collect and subsequently transfer data over a network without human interaction. *Watson Internet of Things: What is the IoT?*, IBM, <https://www.ibm.com/internet-of-things/learn/what-is-iot/> (last visited Nov. 10, 2018).

7. Yiftah Ben Aharon, *Small Wearable Devices May Lead to Big Health Care Savings*, STAT (June 7, 2017), <https://www.statnews.com/2017/06/07/wearable-devices-health-care-savings/>.

8. *Internet of Things*, WIKIPEDIA, https://en.wikipedia.org/wiki/Internet_of_things (last updated Nov. 8, 2018).

A. Market Usage and Adoption

Though wearables were originally designed to support medical needs, the market experienced an increase in the past decade in devices designed to assist recreational users in tracking health and fitness levels.⁹ Thus, wearables include sensors that monitor and record not only sensitive patient health information (e.g., blood pressure, respiratory rate, oxygen saturation, temperature, etc.),¹⁰ but also daily recreational physical activity¹¹ (e.g., steps taken, distance traveled, calories burned, sleep patterns, heart rate, etc.).¹² Perhaps the most well-known recreational wearables are fitness activity bands and smart watches (e.g., Fit-bit, Apple Watch, Garmin, Nike Fuelband, etc.). Across both applications, wearables are revolutionizing health care by generating accessible real-time personal health information.

Today, the market is flooded with both medical and recreational wearables¹³ and trends suggest their popularity is likely to continue. Nearly one-in-five Americans own a wearable¹⁴ and experts predict the devices will eventually become “as ubiquitous as cell phones.”¹⁵ Global revenue from wearables is projected to grow at a compound average growth rate¹⁶ of 29%¹⁷ to reach more than \$6.3 billion by 2020—a dramatic increase from the \$218 million in 2015.¹⁸ Wearables are also attracting a significant level of interest from investors, who invested

9. Langley, *supra* note 3, at 1644; *see also* Troiano, *supra* note 1, at 1716.

10. Grant Arnow, *Apple Watch-ing You: Why Wearable Technology Should Be Federally Regulated*, 49 LOY. L.A. L. REV. 607, 608 (2016); *see also* Langley, *supra* note 3, at 1644.

11. Langley, *supra* note 3, at 1643–44.

12. Aharon, *supra* note 7.

13. Janice Phaik Lin Goh, *Privacy, Security, and Wearable Technology*, LANDSLIDE, Nov./Dec. 2015, at 30.

14. Langley, *supra* note 3, at 1645.

15. Sarah Kellogg, *Every Breath You Take: Data Privacy and Your Wearable Fitness Device*, 72 J. MO. B. 76, 77 (2016).

16. A compound average growth rate is the mean annual growth rate of an investment over a specified period longer than one year. *Compound Annual Growth Rate – CAGR*, INVESTOPEDIA, <https://www.investopedia.com/terms/c/cagr.asp> (last visited Nov. 10, 2018).

17. *Global Wearable Technology Market Growth, Analysis, Size and Forecast 2030 by Applications in Healthcare, Fitness and Communication Industry*, REUTERS (Nov. 7, 2017, 9:00 AM), <https://www.reuters.com/brandfeatures/venture-capital/article?id=20114>.

18. Vera Gruessner, *Wearable Devices Market Expected to Reach \$6.3 Billion by 2020*, MHEALTH INTELLIGENCE (Oct. 19, 2015), <http://mhealthintelligence.com/news/wearable-devices-market-expected-to-reach-6.3-billion-by-2020>; *see also* Troiano, *supra* note 1, at 1716.

nearly \$41 million in development and marketing of the devices between 2008 and 2014.¹⁹ These projections suggest wearables will become and remain a popular consumer product in society and command substantial attention from both a commercial and legal standpoint.

B. The Benefits of Wearables

Wearables and associated health data transferred to companion applications present a variety of social opportunities and benefits. Perhaps most importantly, wearables have the potential to reduce health care costs by improving individual well-being and generating associated data analytics that medical and non-medical third-parties can leverage for a variety of commercial purposes. A significant portion of the country's rising health care cost is driven by unhealthy behaviors (e.g., poor diet, little exercise, stress, excessive alcohol consumption, smoking, etc.), many of which frequently lead to more serious and chronic diseases (e.g., obesity, diabetes, heart disease, etc.).²⁰ These conditions collectively account for nearly 86% of all health care expenses.²¹ To combat such trends, policymakers are attempting to improve both the health of populations and experience of care, while simultaneously reducing the per capita cost.²² Proactively engaging patients in their own health—ideally, before unhealthy behaviors lead to more chronic diseases—is central to achieving these objectives,²³ and wearables may be an effective tool in that effort.

Individual well-being could be improved using wearables since their convenience and diagnostic capabilities may enable users to effectively monitor health and identify potential medical problems at an earlier stage.²⁴ Since personal health data is constantly being collected from wearables and processed via companion applications, users can immediately access data compilations and analyses in one place²⁵ with

19. Matt Witheiler, *The Investments in a Wearables Future*, TECHCRUNCH (Sep. 20, 2014), <https://techcrunch.com/2014/09/20/the-wearable-future/>.

20. Parmy Olson, *Wearable Tech Is Plugging into Health Insurance*, FORBES (June 19, 2014, 1:26 PM), <https://www.forbes.com/sites/parmyolson/2014/06/19/wearable-tech-health-insurance/#621a6e4618bd>.

21. Aharon, *supra* note 7.

22. Nicolas P. Terry, *Will the Internet of Things Transform Healthcare?*, 19 VAND. J. ENT. & TECH. L. 327, 329 (2016).

23. *Id.*

24. Goh, *supra* note 13, at 32.

25. Troiano, *supra* note 1, at 1716.

virtually no effort.²⁶ This detailed stream of personal health information may—when regularly reviewed—promote healthier behavior among users²⁷ because it reminds users of the long-term impact of poor lifestyle choices.²⁸ For example, recreational wearables often help highlight sedentary habits by reminding users to stand after extended periods of sitting²⁹ or to walk a certain number of steps each day. Access to these and other previously unmeasurable metrics³⁰ makes it easier for users to consciously engage with their health, effectively moving society closer toward the ultimate objective of reducing health care costs.³¹

Medical wearables may also facilitate an increased interest in preventative care³² among health care providers, rather than traditional reactive treatments of more serious later-stage conditions.³³ Common methods of such care—which arguably reduce the overall cost of treatment in the long-run—include self-examinations, regular health check-ups, disease screenings, maintaining updated immunizations, etc.³⁴ Similar to these strategies, wearables may become another channel of preventative care since certain data generated—if disclosed and monitored—could alert health care providers of problems requiring more immediate attention³⁵ or inform providers more holistically of a patient’s lifestyle and health profile. For example, wearables could make it easier for users and health care providers to detect and treat influenza.³⁶ Symptoms for the disease, whether mild or severe, often

26. Arnow, *supra* note 10, at 608.

27. Troiano, *supra* note 1, at 1716.

28. Arnow, *supra* note 10, at 610.

29. *Id.*

30. *Id.* at 607–08.

31. According to a survey conducted by Price Waterhouse Coopers, nearly 56% of respondents believed that wearables could extend their life expectancy by ten years while 46% thought wearables could decrease obesity by helping consumers more effectively monitor nutrition and exercise. *Healthy Wearables: Early Days*, 1 PWC 11, 1 (2014), <http://www.healthworkscollective.com/wp-content/uploads/2016/04/pwc-hri-wearable-devices.pdf>.

32. Though its effectiveness is still a topic of debate, preventative care emphasizes disease prevention through early identification and proactive treatment of potential health problems. *Preventative Healthcare*, WIKIPEDIA, https://en.wikipedia.org/wiki/Preventive_healthcare (last updated Oct. 8, 2018).

33. Goh, *supra* note 13, at 32.

34. *Id.*

35. Aharon, *supra* note 7.

36. Andrew Boyd, *Could Fitbit Data Be Used to Deny Health Coverage*, U.S. NEWS (Feb. 17, 2017, 1:26 PM), <https://www.usnews.com/news/national-news/articles/2017-02-17/could-fitbit-data-be-used-to-deny-health-insurance-coverage>.

are difficult to recognize, and certain treatments are most effective only if administered within twenty-four hours of their onset.³⁷ A wearable could identify the presence of this condition almost immediately if it measured “a sudden decrease in the number of steps the person takes per day” along with “an elevated resting heart rate.”³⁸ Also, data analytics collected from wearables over an extended period could assist health care providers in more accurately diagnosing problems and prescribing treatments for patients.³⁹ The data could even be synced with electronic health records to enable greater patient accountability, which could potentially lead to reduced patient readmission costs.⁴⁰ Such readmissions are not only expensive, but also avoidable if the hospital improves its discharge process to facilitate enhanced patient self-management.⁴¹

Since comprehensive preventative care is often too expensive for health systems and patients,⁴² certain features of wearables could serve as an ancillary form of care. A need for medical attention, for example, could be triggered if a wearable detected any life threatening patterns (e.g., a heart attack or stroke) of its user.⁴³ While the cost of an appointment with a health care provider varies depending on services rendered and payment method,⁴⁴ the average purchase price of a wearable is only about \$96.03⁴⁵ with limited maintenance and operating

37. *Id.*

38. *Id.*

39. Research by Accenture suggests that 63% of patients are open to sharing wearable data with their health plans and 90% are willing to share that data with medical providers. Bruce Japsen, *How Insurers and Wearables Will Change Healthcare*, MOTLEY FOOL (Mar. 13, 2016, 2:02 PM), <https://www.fool.com/investing/general/2016/03/13/how-insurers-and-wearables-will-change-healthcare.aspx>.

40. Troiano, *supra* note 1, at 1720. A readmission is “an inpatient stay that begins within 30 days of the discharge date of an index admission and can be to the same or a different hospital” and “may or may not be related to the care received at the index admission.” Gregory Johnson, *The Cost of a Hospital Readmission*, LINKEDIN (Jan. 16, 2017) (citation omitted), <https://www.speechmed.com/cost-hospital-readmission/>. A recent study estimated the following average costs of a readmission for patients receiving: Medicare (\$13,800), Medicaid (\$12,300), uninsured persons (\$10,100), and private insurer (\$14,200). *Id.*

41. *Id.*

42. *Preventative Healthcare*, *supra* note 32.

43. Timothy L. Fort et. al., *The Angel on Your Shoulder: Prompting Employees to Do the Right Thing Through the Use of Wearables*, 14 NW. J. TECH. & INTELL. PROP. 139, 149 (2016).

44. In 2011, the average cost of a fifteen minute visit with a doctor was \$104. *Doctor Visit Costs*, DEBT.ORG, <https://www.debt.org/medical/doctor-visit-costs/> (last updated May 24, 2018).

45. The average purchase price of “health and fitness trackers” was estimated by Statista

costs thereafter—assuming the user has access to a smartphone or computer to view the data compiled on a companion application.⁴⁶ If wearables prove to be an adequate supplement to preventative care, the devices could provide substantial savings for individuals looking to reduce their reliance upon expensive health care providers.

In addition to preventative care, precision medicine⁴⁷ provides customized medical treatment to patients based on individual characteristics. Under this approach, providers offer optimal patient treatments based on an individual's genetics, environment, and lifestyle.⁴⁸ Wearables could help in this effort since more comprehensive patient monitoring would likely create more complete datasets to aid in identifying useful subgroups for patient profiling.⁴⁹ When detailed genetic information is combined with phenotypic data generated by wearables, providers are better equipped to “identify the right patients to receive the right therapy at the right time.”⁵⁰ Thus, wearables coupled with preventative care and precision medicine not only have the potential to improve individual well-being, but also to “revolutionize disease treatment.”⁵¹ As such, it is not surprising that wearables are being “touted as the revolution in health care.”⁵²

If disclosed, data generated by wearables could also be leveraged by non-medical third-parties—including employers-at-large, insurance providers, marketers, and even lawyers—in ways that may also reduce health care costs. Categorically speaking, each of these entities

in 2014 to be £73, which converts to approximately \$96.03 USD. *Average Price of Wearable Technology Products in the United Kingdom (UK) Between January and September 2014 (in GBP)*, STATISTA, <https://www.statista.com/statistics/373766/wearables-technology-average-product-price-uk-united-kingdom/> (last visited Nov. 10, 2018).

46. In 2017, smartphone penetration in the U.S. reached 69.3%. *Top 50 Countries/Markets by Smartphone Users and Penetration*, NEWZOO (Sept. 2018), <https://newzoo.com/insights/rankings/top-50-countries-by-smartphone-penetration-and-users/>.

47. Precision medicine is “an emerging approach for disease treatment and prevention that takes into account the individual variability in genes, environment, and lifestyle for each person.” *What Is Precision Medicine?*, GENETICS HOME REFERENCE (Oct. 23, 2018), <https://ghr.nlm.nih.gov/primer/precisionmedicine/definition>.

48. Arnov, *supra* note 10, at 612-13.

49. David Shaywitz, *Wearables as Tools for Precision Medicine: Promise in Search of Evidence*, FORBES (Feb. 7, 2015, 8:43 PM), <https://www.forbes.com/sites/davidshaywitz/2015/02/07/wearables-as-tools-for-precision-medicine-a-promise-in-search-of-evidence/#15d2ef10477a>.

50. *Id.*

51. “Precision medicine promises to improve health and revolutionize disease treatment by accelerating biomedical discoveries, providing clinicians with new tools, knowledge, and therapies to select effective treatments for individual patients.” Arnov, *supra* note 10, at 612-13.

52. Goh, *supra* note 13, at 32.

is already harnessing wearable data to incentivize desired behavior and enhance market efficiencies. A popular practice among employers, for example, is the implementation of corporate health and wellness programs that invite employees to track their health habits using wearables.⁵³ Today, nearly 90% of companies in the United States offer some form of corporate wellness program.⁵⁴ Most of these aim to improve employee health and maximize workplace productivity while minimizing costly medical and insurance expenses.⁵⁵ Many employers have taken these programs a step further by partnering with insurance providers willing to grant employees discounts for participation in their health-tracking programs.⁵⁶ Under the Affordable Care Act, employers may offer wellness incentives (e.g., gift cards, rate discounts, etc.) to employees—paid for by the insurance providers—as long as employees use a wearable that records their daily activity.⁵⁷ UnitedHealthcare, for example, has offered participating employees up to \$4.00 per day for meeting certain daily walking goals.⁵⁸

Even without an employer wellness program, insurance providers recognize the value of wearables and have found ways to integrate them into individual policyholder plans.⁵⁹ Data generated by weara-

53. Scott Thiel & Nicolas Boyle, *Wearables at Work: Data Privacy and Employment Law Implications*, DLA PIPER (Apr. 22, 2016), <https://www.dlapiper.com/en/us/insights/publications/2016/04/wearables-at-work/>.

54. *Id.*

55. *Id.* For example, Tokyo Electron, a Japanese semiconductor manufacturer, estimated it would pay \$3200 per employee annually if the company had not implemented a wellness program using Fitbits. Within eight years of implementing the program, Tokyo Electron found that the number of annual claims by employees was effectively reduced 6%—a claim is a request for payment that an individual (or that individual's health care provider) submits to their health insurance provider when health services provided fall within coverage of the insurance policy of the individual. Troiano, *supra* note 1, at 1721–23; *see also* Olson, *supra* note 20.

56. Lindsey Patterson, *6 Insurance Companies Investing in Wearable Technology*, TECHZONE 360 (June 27, 2016), <http://www.techzone360.com/topics/techzone/articles/201606/27/422510-6-insurance-companies-investing-wearable-technology.htm#>.

57. Between 60-85% of employees are willing to share their health information with employers to receive discounts on their premiums. Christina Farr, *Weighing Privacy Vs. Rewards of Letting Insurers Track Your Fitness*, NPR (Apr. 9, 2015, 7:08 AM), <https://www.npr.org/sections/alltechconsidered/2015/04/09/398416513/weighing-privacy-vs-rewards-of-letting-insurers-track-your-fitness>.

58. Aharon, *supra* note 7.

59. A global survey by Accenture found that 63% of insurance executives believe wearables will be broadly adopted by the industry within the next two years with nearly a third already using the devices to engage customers, employers, and partners. Denise Johnson, *How Wearable Devices Could Disrupt the Insurance Industry*, INSURANCE JOURNAL (May 6, 2015), <https://www.insurancejournal.com/news/national/2015/05/06/367014.htm>.

bles, for example, can help providers conduct more accurate evaluations of potential policyholders and simultaneously promote healthier behaviors among current ones.⁶⁰ Traditionally, insurance providers base policy underwriting⁶¹ on a limited set of available variables (e.g., age, body mass index, etc.) with rates calculated through annual lifestyle risk assessments (e.g., frequent skydiving would likely equate to a higher insurance premium).⁶² Wearables, however, present an unprecedented opportunity for carriers to underwrite based on the daily activity of policyholders for more accurate behavioral-based rates.⁶³ In other words, policyholders who exhibit a healthy lifestyle would be rewarded with a lower premium—much in the same way embedded devices in vehicles are being used to reward policyholders for safe driving in the automobile insurance industry.⁶⁴ On the other hand, policyholders with poor health habits (or those who simply fail to provide their personal data) could be assessed higher premiums as they would present a greater financial risk to the insurance provider.⁶⁵ Experts predict that insurers will soon begin leveraging wearables to calculate premiums on a more real-time basis—that is, replacing stagnant annual insurance rates under the current model with daily insurance rates based on individual actions.⁶⁶ Proponents of these underwriting changes suggest insurance providers will reduce health care costs as policyholders become more accountable for unhealthy behaviors and are incentivized to make appropriate lifestyle changes.⁶⁷

60. Troiano, *supra* note 1, at 1723; *see also* Lucas Mearian, *Insurance Company Now Offers Discounts—If You Let It Track Your Fitbit*, COMPUTERWORLD (Apr. 17, 2015, 12:34 PM), <https://www.computerworld.com/article/2911594/insurance-company-now-offers-discounts-if-you-let-it-track-your-fitbit.html>.

61. “Underwriting is the process of evaluating the risk of insuring a home, car, driver or individuals, such as in the case of life insurance, to determine if it’s profitable for the insurance company to take the chance. After determining the risk, the underwriter sets a price and establishes the insurance premium that will be charged in exchange for taking on that risk.” Mila Araujo, *What is Insurance Underwriting*, BALANCE (Oct. 28, 2018), <https://www.the-balance.com/what-is-insurance-underwriting-2645778>.

62. Troiano, *supra* note 1, at 1723; *see also* *Finding Insurance Insider Information: How Insurance Companies Measure Risk*, INSURANCE COMPANIES.COM, <http://www.insurancecompanies.com/insider-information-how-insurance-companies-measure-risk/> (last visited Nov. 10, 2018).

63. Jo Best, *Yes, Insurers Want Your Health Data - but Not for the Reason You Think*, ZDNET (Nov. 3, 2015, 10:15 PM), <https://www.zdnet.com/article/yes-insurers-want-your-health-data-but-not-for-the-reason-you-think/>.

64. Patterson, *supra* note 56.

65. Troiano, *supra* note 1, at 1723.

66. Olson, *supra* note 20.

67. *Id.*

Data generated by wearables is also being leveraged by marketing professionals and lawyers for industry specific purposes. Marketers use data to better understand and cater to consumer preferences. With a more holistic view of consumers, these professionals can develop highly personalized experiences⁶⁸ and provide more targeted product offerings.⁶⁹ A clothing company, for example, could promote tighter fitting clothing to a user whose wearable reported significant weight loss.⁷⁰ Similarly, a mattress company could advertise the benefits of a new mattress to a user whose wearable registered poor sleep.⁷¹ These and other strategies could enhance consumer marketplace efficiencies. Wearable data is also becoming increasingly valuable to lawyers as a form of evidence and discovery. Although the rules of admissibility of such data remain in question, wearable data has already been accepted by some courts.⁷² In a world where data is like currency, the benefits and opportunities associated with wearables and their accompanying data are almost endless. By improving the personal health awareness of users and generating valuable analytics for medical and non-medical third-parties, wearables could be a driving force in reducing the cost of health care.

C. The Drawbacks of Wearables

Despite the foregoing potential benefits, wearables do not come without a cost and are accompanied by several significant drawbacks. Some of the most concerning challenges include questionable device utility, data breach threats, and potential discriminatory applications of generated data. Since personal health information is perhaps the

68. Experts predict that soon we will see fabrics that can react to electric charge to change color, enabling users to control light patterns to match other elements in their outfit or colors in the surrounding environment. Zac Pinkham, *How Will Wearables Influence Mobile Advertising*, MARKETINGTECH (July 17, 2015), <https://www.marketingtechnews.net/news/2015/jul/17/how-will-wearables-influence-mobile-advertising/>.

69. Langley, *supra* note 3, at 1646.

70. *Id.*

71. *Id.*

72. In Canada, a plaintiff used her wearable data (i.e., a detailed record of gym visits before and after the accident) to prove a decline in physical activity after sustaining an injury in a car accident, which allowed her to prevail on her claims. Angela Foster, *Legal Implications of Data from Wearable Devices*, ABA (Apr. 3, 2017), <https://www.americanbar.org/publications/litigation-news/technology/legal-implications-of-data-from-wearable-devices.html>.

most sensitive data type in existence,⁷³ users and third-parties collecting, analyzing, and publishing wearable data should carefully consider these challenges when leveraging a device or its associated data.

Wearables have been fundamentally criticized for a lack of utility primarily due to ineffectiveness and inconsistency. Primarily, these criticisms derive from alleged unreliability of generated data and a lack of evidence that wearable usage truly alters behavior for the better. A growing body of research suggests that existing wearable models are not especially effective at collecting accurate data.⁷⁴ Such inconsistencies become especially problematic when employers and insurance providers rely upon device data to calculate rewards and insurance premiums. Recent comparisons, for example, between different wearables tracking identical user activity revealed substantial variations⁷⁵ in data accuracy—with error margins upwards of 25%.⁷⁶ If perfect device accuracy is presumed to be unlikely, employers and insurance providers would face the daunting task of determining what the acceptable error margin should be for devices incorporated into their programs. Additional concerns surround potential user ability to trick the device into tracking false information or to manipulate the collected data thereafter. Is there any mechanism in place, for example, to prevent a user from paying the local paperboy to wear their device around the neighborhood each morning to earn extra miles? Likewise, users may frequently fail to charge, sync, or wear their devices, effectively preventing data from being accurately collected at crucial moments in time.⁷⁷ If attractive enough incentives are offered to users, employers and insurance providers should reasonably expect participants in their programs to find fraudulent avenues for achieving the preferred standards.

Even if wearables could generate accurate data, most device manufacturers are still unable to provide any empirical evidence that their

73. Troiano, *supra* note 1, at 1724.

74. Terry, *supra* note 22, at 335.

75. According to Dr. Douglas Ross, an Intermountain Healthcare pulmonologist, wearables “often overestimate sleep time and cannot accurately determine sleep quality.” Aley Davis, *Smartwatch Helps Mom of Five Track Her Sleep, but Is the Device Helpful?*, KSL.COM (May 3, 2018, 6:28 PM), <https://www.ksl.com/?sid=46312968&nid=148&title=smartwatch-helps-mom-of-five-track-her-sleep-but-is-the-device-helpful>.

76. Jung-Min Lee, Youngwon Kim & Gregory J. Welk, *Validity of Consumer-Based Physical Activity Monitors*, 46 J.MED. & SCI.IN SPORTS & EXERCISE 1840, 1840 (2014); *see also* Meredith A. Case, Holland A Burwick, Kevin G. Volpp & Mitesh S. Patel, *Accuracy of Smartphone Applications and Wearable Devices for Tracking Physical Activity Data*, 313 J. AM. MED. ASS’N 625, 625–26 (2015).

77. Fort, *supra* note 43, at 153–54.

products are truly effective in changing behavior. Though only a limited amount of research exists regarding wearable effectiveness,⁷⁸ most reports suggest wearables do little to incentivize behavioral change among users.⁷⁹ In a recent year-long study, researchers measured the health and physical activity of 800 individuals with full-time jobs—some wore a Fitbit and were paid a small amount of money to exercise, while others were instructed not to wear a Fitbit.⁸⁰ During the last six months of the study, all monetary incentives were dropped and participants could choose whether to continue wearing their device.⁸¹ While monetary incentives seemed to work,⁸² improvements ceased as soon as the rewards were eliminated.⁸³ No group successfully improved their health outcomes measured by the researchers for either six or twelve months.⁸⁴ The lead researcher ultimately concluded that wearables “should not be relied upon as tools for weight management in place of effective behavioral counseling for physical activity and diet.”⁸⁵ In other words, simply giving an individual a wearable that tracks their health behaviors against what they should be doing is not particularly motivating.⁸⁶ Though some suggest any increase in physical activity is beneficial, the author of the study argues that minor increases are not enough to produce meaningful change.⁸⁷ As it turns out, motivating individuals to adopt healthy habits is extremely difficult to do⁸⁸—even if you pay them to do it—and wearables may not be enough “to motivate the people who need to be motivated the most.”⁸⁹

78. Bryan Bumgardner, *Do Fitness Wearables Live Up to Their Promise?*, CBS NEWS (June 24, 2015, 10:27 AM), <https://www.cbsnews.com/news/do-fitness-wearables-live-up-to-their-promise/>.

79. Mandy Oaklander, *There's Even More Evidence That Fitness Trackers Don't Work*, TIME (Oct. 4, 2016), <http://time.com/4517033/fitness-tracker-fitbit-zip-exercise/>.

80. *Id.*

81. *Id.*

82. Those rewarded with cash performed an additional thirteen minutes of moderate-to-vigorous physical activity each week, effectively adding 570 steps to their daily counts. *Id.*

83. *Id.*

84. *Id.*

85. *Activity Trackers Are Ineffective at Sustaining Weight Loss*, SCIENCE DAILY (Sept. 20, 2016), <https://www.sciencedaily.com/releases/2016/09/160920131932.htm>.

86. Oaklander, *supra* note 79.

87. *Id.*

88. *Id.*

89. Bumgardner, *supra* note 78.

Similarly, additional research suggests that a principal reason behind the lack of motivation to adopt health habits is the failure of wearables to drive long-term interest and engagement among users. One survey found that a third of users stopped using their devices within six months of receiving them and nearly half stopped within a year.⁹⁰ A surprisingly high percentage of users stopped using their devices because they experienced one or more fatal user experience flaws⁹¹ (e.g., easily lost or broken, too difficult to sync with other devices, poor battery life, displeasing aesthetics, discomfort to the user, etc.).⁹² Others may be discouraged altogether from using wearables by health professionals if the devices cause users too much stress.⁹³ Moreover, wearables fail to track a significant component of personal health—that is, food consumed by a user. Regardless of an individual’s level of physical activity, their health is still largely dependent upon “what food [they] put into [their] bod[ies].”⁹⁴ Though everyone seems to be looking for an easy fix to poor health habits and high health care costs, the metrics measured by wearables alone are not what will actually make individuals healthy.⁹⁵ Thus, device manufacturers hoping to make a meaningful impact should continue exploring alternative ways to motivate users, resolve user experience obstacles, and account for food consumption.

90. *Id.*; see also Teena Maddox, *Wearables Have a Dirty Little Secret: 50% of Users Lose Interest*, TECHREPUBLIC (Feb. 13, 2014, 12:29 PM), <https://www.techrepublic.com/article/wearables-have-a-dirty-little-secret-most-people-lose-interest/>.

91. Dan Ledger & Daniel McCaffrey, *Inside Wearables: How the Science of Human Behavior Change Offers the Secret to Long-Term Engagement*, MEDIUM (Jan. 2014), <https://blog.endeavour.partners/inside-wearable-how-the-science-of-human-behavior-change-offers-the-secret-to-long-term-engagement-a15b3c7d4cf3>.

92. Maddox, *supra* note 90.

93. According to Dr. Douglas Ross, an Intermountain Healthcare pulmonologist, if wearables cause stress they are probably not worth it: “[t]he more they worry about their sleep and their insomnia, the more they stress . . . [a]nd the more they worry, the less sleep comes.” Davis, *supra* note 75.

94. Bumgardner, *supra* note 78.

95. *Id.*

A second alarming challenge associated with wearables is data breach, which may be partially due to information asymmetries between users and device manufacturers.⁹⁶ The risk of data breach⁹⁷ is especially concerning given the sensitive nature of personal health information and relatively unsound practices of wearable data collection and dissemination. Data generated by wearables is considered by many to be even more sensitive and vulnerable than financial data.⁹⁸ Certain procedures and diagnoses, for example, often become a permanent part of a patient's medical history.⁹⁹ If accessed even once by a hacker,¹⁰⁰ health information can be mishandled and used against an individual forever (e.g., sold to companies that could build user profiles without consumer consent, collected by stalking applications, etc.).¹⁰¹ Equally concerning is the unsound collection and dissemination of wearable data, which users often have little control over due to information asymmetries. Most users, for example, expect wearables to collect data on steps taken and sleeping patterns, but are often unaware that devices also collect precise geolocation data—which could reveal highly personal information (e.g., an individual's visit to an AIDS clinic or place of worship).¹⁰² Similarly, wearables often continue collecting data, unbeknownst to users, even after the battery of the device dies or a user

96. Advocates for greater user protection argue that most people care about data privacy, but simply do not know how to use the Internet and other related technologies in ways that simultaneously protect their data (e.g., users are uncertain as to how their data is being used and transmitted since the backend functionality of wearables is often hidden). Kellogg, *supra* note 15, at 79–80. Yet, those purchasing wearables seem to consistently place a higher value on device convenience and ease of use rather than added security features that would undoubtedly increase purchase price. Sharon D. Nelson, *Advances Will Keep Transforming Our Lives—and Threaten Privacy, Security*, 40 MONT. L. 18, 22 (2015).

97. The Identify Theft Research Center predicted that the number of data breaches in the United States would reach nearly 1500 in 2017, a 37% increase from the prior year. Nick Ismail, *Should the US Adopt GDPR?*, INFO. AGE (Nov. 7, 2017), <https://www.information-age.com/us-adopt-gdpr-123469401/>. Yet, data privacy remains relatively unregulated across the nation. *Id.*

98. According to Michelle De Mooy, Deputy Director of the Consumer Privacy Project at the Center for Democracy & Technology, personal health information generated by wearables is even more vulnerable than financial data “because you can’t replace it like you can a credit card.” Kellogg, *supra* note 15, at 76.

99. *Id.*

100. “According to a recent YouGov survey, 28% of U.S. adults admit to using the same password for all or most of their online logins, which is even more astonishing considering that 35% of the respondents had one of their accounts hacked at least once and 22% have fallen victim to online identity theft.” Felix Richter, *Young Americans are Careless With Their Online Passwords*, STATISTA (Oct. 18, 2017), <https://www.statista.com/chart/11525/americans-using-the-same-online-password/>.

101. Goh, *supra* note 13, at 31.

102. *Id.*

closes a companion application.¹⁰³ This collected data is frequently “stored within vulnerable network systems, the security of which is largely, if not entirely, unregulated.”¹⁰⁴ In other words, users are generating a tremendous amount of data, but wearable companies do not “tak[e] some of the necessary precautions that more established companies would take in terms of data privacy and security.”¹⁰⁵ Multiple device and platform integration only heightens the risk of data breach since “the least secure device becomes the security level for all [the devices].”¹⁰⁶ Even if companies were to incorporate additional security features, “no data is immune from a breach”¹⁰⁷ and its permanent deletion is often “difficult (if not impossible)” to remedy.¹⁰⁸ Given these realities, it is not surprising that Americans often feel they have little control over the information collected about them and ignorantly presume “their data will in fact remain private and secure.”¹⁰⁹

Perhaps most disheartening, is that wearables could threaten individual privacy and lead to potential discriminatory applications of the generated data. At first glance, wearables seem like an optimal solution for reducing health care costs since they are positioned to incentivize people to develop healthier lifestyles. An incentive structure built around individual habits, however, has potential to unfairly advantage and disadvantage certain subsets of the population. Debate exists, for example, over whether wearables truly serve the population at large or if they simply cater to the already healthy and wealthy.¹¹⁰ A recent report indicated that nearly 41% of fitness tracker owners earned an average annual income of more than \$100 thousand.¹¹¹ Thus, behavioral

103. Troiano, *supra* note 1, at 1724–25.

104. Arnow, *supra* note 10, at 615.

105. Kellogg, *supra* note 15, at 77.

106. *Id.* at 78.

107. Farr, *supra* note 57 (according to Christine Sublett, a Silicon Valley-based security expert).

108. Arnow, *supra* note 10, at 613.

109. Mary Madden & Lee Rainie, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CENTER (May 20, 2015), <http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.

110. Lukasz Piwek, David A. Ellis, Sally Andrews & Adam Joinson, *The Rise of Consumer Health Wearables: Promises and Barriers*, PLOS MED. (2016), <https://journals.plos.org/plosmedicine/article?id=10.1371/journal.pmed.1001953>.

111. The federal poverty level in 2017 was \$12,060 for households with one person living within the forty-eight Border States and Washington, D.C. Lindsay Wissman, *2017 Federal Poverty Level Guidelines*, PEOPLEKEEP (Feb. 7, 2017), <https://www.peoplekeep.com/blog/2017-federal-poverty-level-guidelines>.

economists argue that adoption of the devices may implicitly bias low-income individuals.¹¹² Those working several part-time jobs, for example, may be so limited financially that they are unable to purchase and prepare healthy foods, access adequate exercise facilities, or even set aside time for any exercise at all.¹¹³ Overtime, it is reasonable to expect that the personal health profiles—which would include historical and real-time wearable data—of these low-income individuals would look drastically different from those living in greater abundance.¹¹⁴ In turn, these discrepancies could compel low-income individuals to pay higher premiums.¹¹⁵ Such a discrepancy between income classes is troubling when considering how profiles may affect individual access or cost to obtain insurance coverage.

Insurance providers with access to voluntarily disclosed personal health profiles could also create more accurate and customized risk-based policies for their insured. Today, such data is rarely used at the individual level to calculate potential risk—though, personalized behavioral-based coverage assessments are certainly within the realm of possibility with wearables. Instead, many insurance carriers estimate risk levels through sophisticated models that combine vast non-personal data to predict individual risk (e.g., assuming a male between thirty and forty years old is likely low risk based on previously aggregated data on men that age).¹¹⁶ The voluntarily shared wearable data from individuals to employers and insurance providers is precise enough to ultimately fuel large-scale algorithmic models. While most classify the exchange as a reward, privacy experts fear it is “ultimately a stick” disguised as a carrot.¹¹⁷ In other words, experts foresee carriers aggregating such voluntarily disclosed wearable data—most, if not all, of which was acquired lawfully through optional participation incentive programs—to develop large datasets that could be used to identify trends and eventually deny coverage to individuals based on their algorithmically estimated health risks.¹¹⁸ Even those unwilling to voluntarily disclose their wearable data could then be discriminated against

112. Farr, *supra* note 57.

113. *Id.*

114. Olson, *supra* note 20.

115. *Id.*

116. Alan Martin, *Step and Save: The Truth About Wearables and Health Insurance*, WEARABLE (May 21, 2015), <https://www.wearable.com/wearable-tech/step-and-save-the-risks-of-using-fitness-tracker-to-save-on-your-insurance-premium-1163>.

117. Farr, *supra* note 57.

118. Boyd, *supra* note 36.

by insurers, who could apply the aggregated data of similarly situated persons to such individuals.¹¹⁹ Like a low credit score, unhealthy habits could place individuals a “blacklist”¹²⁰ which could allow insurance providers to raise premiums for those unwilling or unable to get healthier. While this would certainly introduce a compelling incentive system, it is concerning to think of health insurance functioning like car insurance—where any health infraction (e.g., holiday feast, sedentary Netflix binge, etc.) could hurt your real-time health score.¹²¹ Generally, insurance companies are only allowed to increase the premiums of their insured by showing the individual exhibited “increased risk.”¹²² If read too broadly, however, an increased risk could be almost anything (e.g., walking through a dangerous area, cycling or skiing too fast, etc.) as the insurance industry moves closer toward its “data-driven future.”¹²³ Though we are likely years away from this dystopian nightmare, many believe society is on its way there.¹²⁴

Mandated use of wearables and/or disclosure of their resulting data would only worsen the consequences of discrimination. As history has shown, voluntary programs today—like disclosure of wearable data for rewards—could easily become mandatory in the future.¹²⁵ Employers could force employees to use wearables and regularly report their results. Insurance providers could require prospective policyholders to

119. If an insurance provider, for example, aggregated enough information about people with asthma, they could likely detect an asthma patient “looking just at their data.” *Id.*

120. Farr, *supra* note 57.

121. Cindy Ng, *What If Fitness Wearables Affected Our Health Insurance Rates*, VARONIS (Mar. 12, 2015), <https://blog.varonis.com/fitness-wearables-affected-health-insurance-rates/>.

122. Ben Lovejoy, *John Hancock Requires Vitality Program Membership; Sharing Fitness Data Earns Rewards*, 9TO5MAC (Sept. 20, 2018), <https://9to5mac.com/2018/09/20/john-hancock-life-insurance-apple-watch/>. John Hancock—a prominent life insurance company—recently announced that all new policyholders will be required to join its Vitality program, which requires the recording of fitness and health data using wearable devices. *Id.* The insurer will also be converting existing policies to its Vitality program at the start of next year. *Id.* Though the actual sharing of data with John Hancock continues to remain optional, such strategic underwriting is an example of the insurance industry’s shift toward more “interactive policies.” *Id.*

123. Conor Grant, *156-Year Old Insurer John Hancock Now Requires Customers to Use Health Wearables*, HUSTLE (Sept. 20, 2018), https://thehustle.co/John-Hancock-Life-Insurance-EKG-healthwearables/?utm_campaign=9%2F20%3A+danske+bank&utm_content=John-Hancock-Life-Insurance-EKG-health-wearables&utm_medium=email&utm_source=daily.

124. *Id.*; Lovejoy, *supra* note 122.

125. Initially, “bring your own device” (“BYOD”) workplace initiatives were voluntary opt-in programs, but Gartner estimated that nearly half of employers would mandate BYOD by 2017. Zack Whittaker, *BYOD: From Optional to Mandatory by 2017, Says Gartner*, ZDNET (May 2, 2013, 10:54 AM), <https://www.zdnet.com/article/byod-from-optional-to-mandatory-by-2017-says-gartner/>.

disclose wearable data in place of or in addition to a more traditional physical exam by a health care provider.¹²⁶ Even if wearables were not required to be worn, mere ownership of a device or the apparent willingness to share its data could be revealing enough for an entity seeking to better understand an individual's personal health.¹²⁷ After all, those who own wearables are likely the sort of person an insurer may desire as a policyholder.¹²⁸

Based on the analysis above, the drawbacks of wearables currently seem to outweigh the benefits—thus, entities should be cautious in relying upon wearable data for any meaningful insights. Similarly, policymakers should be thoughtful and avoid creating a system that coerces or even pressures individuals into using wearables to monitor their personal health.¹²⁹ After all, the more society allows for constant tracking, the more difficult it is to prevent technology from “encroach[ing] on our lives.”¹³⁰ Ultimately, the “bad use of data can be worse than no data at all”¹³¹ and the more data entities in power collect, the more it can be used against individuals for gain.

III. EXISTING REGULATORY LANDSCAPE

Despite significant risk surrounding the data they generate, wearables are not currently regulated directly by state or federal statute. Yet, wearables and their accompanying data find some protection—despite their novelty—through a series of other existing legal entities and frameworks.¹³² Several prominent government agencies play a role in helping users protect wearable data from misappropriation and misuse, including the U.S. Department of Health and Human Services (“HHS”), the Food and Drug Administration (“FDA”), the Federal Trade Commission (“FTC”), and the Electronic Communications Privacy Act (“ECPA”).¹³³ A lack of specificity, uniformity, and breadth

126. *Nobody Reads Privacy Policies – Here’s How to Fix That*, CONVERSATION (Oct. 9, 2017, 7:25 PM), <http://theconversation.com/nobody-reads-privacy-policies-heres-how-to-fix-that-81932> [hereinafter *Nobody Reads Privacy Policies*].

127. Best, *supra* note 63.

128. *Id.*

129. Olson, *supra* note 20.

130. Jathan Sadowski, *Why Does Privacy Matter? One Scholar’s Answer*, ATLANTIC (Feb. 26, 2013), <https://www.theatlantic.com/technology/archive/2013/02/why-does-privacy-matter-one-scholars-answer/273521/>.

131. Fort, *supra* note 43, at 168.

132. *Id.* at 1728.

133. *Id.* at 1732.

regarding legal rights protected by these regulatory authorities for wearables, however, often results in inadequate protection of device users' interests. While the Fourth Amendment and legal precedent¹³⁴ grant individuals a reasonable expectation of privacy, those who willingly expose their privacy to the public surrender this fundamental right.¹³⁵ By opting to share their device data with external entities, wearable users often inadvertently renounce this reasonable expectation of privacy. Such disjointed regulatory authority and data privacy laws effectively grant companies in possession of wearable data to control how user data is used—subject only to their own convoluted privacy policies.

A. *The U.S. Department of Health and Human Services*

The HHS, a primary agency of the federal government, aims to promote the health of Americans by providing health and human services and fostering advances in medicine, public health, and social services.¹³⁶ This agency oversees perhaps the most prominent regulation regarding personal health information—the Health Insurance Portability and Accountability Act (“HIPPA”).¹³⁷ Congressional enactment of HIPPA directed the HHS to promulgate regulations to protect both the privacy and security of personal health information.¹³⁸ The HIPPA Privacy Rule established national standards for protecting certain types of health information.¹³⁹ More specifically, the rule limits the use and disclosure of such information without patient authorization and grants various rights to patients about their respective health information (e.g., right to obtain a copy of their health records and request

134. In *Katz v. United States*, the U.S. Supreme Court extended Fourth Amendment protection to include all areas where a person has “reasonable expectation[] of privacy,” yet clarified, “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” *Katz v. United States*, 389 U.S. 347, 351, 362 (1967).

135. Troiano, *supra* note 1, at 1741.

136. *About HHS*, U.S. DEP’T OF HEALTH & HUM. SERVS., <https://www.hhs.gov/about/index.html> (last visited Nov. 10, 2018).

137. *HIPPA Enforcement*, U.S. DEP’T OF HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/index.html> (last visited Nov. 10, 2018).

138. *Summary of the HIPPA Privacy Rule*, U.S. DEP’T OF HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last visited Nov. 10, 2018).

139. *Id.*

corrections).¹⁴⁰ The HIPPA Security Rule effectively operationalized these standards¹⁴¹ by requiring “covered entities”¹⁴² to safeguard any form (i.e., oral, paper, or electronic) of “individually identifiable health information”—which the Privacy Rule calls “protected health information” (“PHI”)—that the entity holds or transmits.¹⁴³ Under the statute, PHI includes any information related to an individual’s “past, present or future physical or mental health or [sic] condition, the provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual”—which often includes demographic information and unique identifiers like an individual’s “name, address, birth date, [and] Social Security Number.”¹⁴⁴ In summary, HIPPA provides an efficient way for covered entities to share PHI electronically in a way that curbs misuse of data and harmful disclosures.

While HIPPA is a broadly applied statute, it is unclear whether wearable manufacturers and the data they collect are regulated by HIPPA. Since wearable manufacturers fall outside the traditional definition of covered entities, they are not clearly subject to HIPPA standards.¹⁴⁵ Similarly, data generated by wearables is not typically viewed or classified as PHI and, therefore, rarely treated as being governed by HIPPA.¹⁴⁶ With that said, manufacturers may be subject to regulations if they voluntarily become HIPPA compliant or find themselves in situations involving a covered entity or in possession of PHI.¹⁴⁷ If a device

140. *Id.*; see also Troiano, *supra* note 1, at 1733.

141. *Summary of the HIPPA Privacy Rule*, *supra* note 138.

142. Covered entities “can be institutions, organizations, or persons” and are defined by HIPPA as health plans (e.g., insurance providers), health care providers (e.g., doctors, clinicians), and health care clearinghouses and their business associates “who electronically transmit any health information in connection with transactions for which HHS has adopted standards.” *To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, NATIONAL INSTITUTES OF HEALTH, https://privacyruleandresearch.nih.gov/pr_06.asp (last visited Nov. 10, 2018).

143. *Summary of the HIPPA Privacy Rule*, *supra* note 138.

144. Troiano, *supra* note 1, at 1732–33. “For example, a medical record, laboratory report, or hospital bill would be PHI because each document would contain a patient’s name and/or other identifying information associated with the health data content.” *Guidance Regarding Methods for De-identification Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U.S. DEP’T OF HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#protected> (last visited Nov. 10, 2018).

145. Troiano, *supra* note 1, at 1732.

146. Adam H. Greene, *When HIPPA Applies to Mobile Applications*, MOBIHEALTHNEWS (June 16, 2011), <https://www.mobihealthnews.com/11261/when-hipaa-applies-to-mobile-applications>.

147. Troiano, *supra* note 1, at 1734.

manufacturer, for example, were granted access to patient health information by a health care provider, the HIPPA standards would likely apply.¹⁴⁸ Companion applications used by covered entities may also receive HIPPA protection.¹⁴⁹ For example, a companion application to a wearable tracking an individual's blood pressure for a health care provider would likely receive HIPPA protection since the collection of such involves both PHI (i.e., information about an individual's physical health condition) and a covered entity (i.e., a health care provider).¹⁵⁰ In contrast, a companion application to a wearable collecting an individual's daily steps is unlikely to receive protection since no covered entity is involved.¹⁵¹ Despite these narrow areas of protection, wearable manufacturers are often unsure as to the breadth of such regulations and may be unwittingly under- or un-regulated by HIPPA given their lack of covered entity status. Although insurance providers are frequently classified as covered entities, HIPPA fails to prevent those entities from obtaining and aggregating wearable data.¹⁵² Thus, HIPPA may prove insufficient to effectively regulate legal challenges associated with wearables-derived personal health information.

B. The Food and Drug Administration

Another federal agency responsible for promoting public health is the FDA. The FDA oversees “the safety and effectiveness of medical devices - including mobile medical apps” that arguably connect to wearables, yet it fails to regulate the proper breadth of wearables.¹⁵³ FDA guidelines¹⁵⁴ issued in 2013, which outlined its oversight respon-

148. 45 C.F.R. § 160.103 (2015); *see also* Troiano, *supra* note 1, at 1734.

149. Greene, *supra* note 146; *see also* Troiano, *supra* note 1, at 1733–34.

150. Troiano, *supra* note 1, at 1733.

151. *To Whom Does the Privacy Rule Apply and Whom Will It Affect?*, *supra* note 142; *see also* Troiano, *supra* note 1, at 1733.

152. Troiano, *supra* note 1, at 1743.

153. *Mobile Medical Applications*, U.S. FOOD & DRUG ADMIN., <https://www.fda.gov/ForConsumers/ConsumerUpdates/ucm255978.htm> (last updated Oct. 8, 2018).

154. “The FDA issued the Mobile Medical Applications Guidance for Industry and Food and Drug Administration Staff on September 25, 2013, which explains the agency’s oversight of mobile medical apps as devices and our focus only on the apps that present a greater risk to patients if they don’t work as intended and on apps that cause smartphones or other mobile platforms to impact the functionality or performance of traditional medical devices.” *Id.*

sibility, primarily emphasized its goal to protect individuals from applications that “don’t work as intended.”¹⁵⁵ In other words, FDA regulations focus almost exclusively on regulating device effectiveness, rather than the privacy of their usage. Additional FDA guidelines¹⁵⁶ released last year reinforce that the agency will not vigorously regulate “low risk devices,” assuming such are “not harmful and generally encourage healthy habits.”¹⁵⁷ Low risk devices may be subject to regulation, however, if considered invasive, implanted, or reliant upon technology that threatens user safety.¹⁵⁸ Since so few wearables pose such risks or meet such requirements, most wearables will likely be classified as low-risk devices and therefore intentionally left unregulated by the FDA.¹⁵⁹ Notably, the FDA is also authorized to regulate medical “devices”¹⁶⁰ as defined by the Federal Food, Drug, and Cosmetic Act. However, wearables are rarely intended to diagnose or cure medical conditions as the definition requires, and accordingly, are unlikely to be governed by such regulation by definition.¹⁶¹ Thus, FDA regulation also comes up short in regulating wearables.

C. The Federal Trade Commission

The FTC is another federal agency involved in consumer protection and is charged with protecting consumers from unlawful trade practices.¹⁶² While the FTC may offer some regulatory protection for

155. *Id.*

156. One such guideline includes the General Wellness: Policy for Low Risk Devices. *General Wellness: Policy for Low Risk Devices – Guidance for Industry and Food and Drug Administration Staff*, 1 U.S. FOOD & DRUG ADMIN. 10, <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm429674.pdf> (last visited Nov. 10, 2018) [hereinafter *General Wellness*].

157. “Many devices with less-than-stellar track records for accuracy – such as calorie counters – would likely not be covered under the guidance.” Colin Lecher, *The FDA Doesn’t Want to Regulate Wearables, and Device Makers Want to Keep It That Way*, VERGE (June 24, 2015, 2:07 PM), <https://www.theverge.com/2015/6/24/8836049/fda-regulation-health-trackers-wearables-fitbit>.

158. *General Wellness*, *supra* note 156, at 5.

159. The FDA provides the following as an example of a device likely to be classified as low-risk: a mobile application that “solely monitors and records daily energy expenditure and cardiovascular workout activities. . . .” *Id.* at 6.

160. The Act defines “device” as instruments “intended for use in the diagnosis of disease or other conditions. . . .” *Is The Product A Medical Device?*, U.S. FOOD & DRUG ADMIN., <https://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm> (last visited Nov. 10, 2018).

161. *Id.*

162. The FTC “works to prevent fraudulent, deceptive, and unfair business practices” and

consumers purchasing and using wearables, the agency generally monitors false or unsupported claims that wearables can diagnose or treat medical conditions.¹⁶³ The FTC does not specifically concern itself with data breaches unless such arises from false or misleading claims associated with the sale of the devices, including those not classified as covered entities. The FTC has recently taken some action, however, to address concerns over a lack of privacy laws governing the devices. The agency, for example, has suggested additional protections addressing consumer privacy threats and advocated for them through workshops and reports.¹⁶⁴ Legal action for data breach could be a means whereby the FTC might protect consumers. Based on available research, however, such actions mostly failed to prevent privacy threats and did nothing to limit insurers from leveraging wearable data in underwriting or evaluating policyholders.¹⁶⁵

Ultimately, such disjointed regulatory authority coupled with a limited patchwork of data privacy laws, allows companies in possession of wearable data to remain largely in control of how generated data is used—often neglecting the interests of users.¹⁶⁶ Such control is only marginally offset by the standard practice among companies to draft expansive privacy notices outlining any limitations that surround their collection and use of user data.¹⁶⁷ More often than not, however, these privacy notices heavily skew toward shielding companies from liability for inadequate data protection.¹⁶⁸ While many unanswered questions remain regarding whether and how the United States government might address this myriad of legal issues presented by wearables—one thing seems clear: that the era of unregulated data is likely coming to an end.¹⁶⁹

“help consumers spot, stop, and avoid scams and fraud.” *Federal Trade Commission*, USA.GOV, <https://www.usa.gov/federal-agencies/federal-trade-commission> (last visited Nov. 10, 2018).

163. *Id.*; see also Troiano, *supra* note 1, at 1737.

164. For example, the FTC has suggested that companion application developers be required to “provide disclosures to users and obtain consent from users when collecting ‘sensitive information.’” Troiano, *supra* note 1, at 1738.

165. The FTC has brought several suits “against companies with allegedly deficient cybersecurity that failed to protect consumer data against hackers,” most of which settled. *Id.* at 1737.

166. Seth P. Berman, *GDPR in the U.S.: Be Careful What You Wish For*, GOVERNMENT TECHNOLOGY (May 23, 2018), <https://www.govtech.com/analysis/GDPR-in-the-US-Be-Careful-What-You-Wish-For.html>.

167. *Id.*

168. *Id.*

169. *America Should Borrow from Europe’s Data-Privacy Law*, ECONOMIST (Apr. 5, 2018), <https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes->

IV. RECOMMENDED SOLUTIONS

As the market for wearables continues to expand, device manufacturers and users alike need practical solutions that both protect consumer privacy and promote technological advancement. Despite a consensus that personal health data be accurately measured and reasonably protected, however, little agreement exists regarding how to balance the promotion of wearable technology and privacy rights. Some privacy advocates suggest the optimal path forward is for America to develop and adopt comprehensive regulation that mirrors a recent European law, known as the GDPR.¹⁷⁰ Broadly speaking, the GDPR¹⁷¹ regulates data protection and privacy for all individuals residing in the European Union.¹⁷² Effective as of May 2018,¹⁷³ this new data privacy law primarily aims to grant individuals greater control over their personal data while simplifying and unifying the regulatory landscape of the region.¹⁷⁴ While in theory, the premise of the GDPR sounds requisite, both its complexity and series of extreme standards, discussed *infra*, make such a regulation ill-suited for application in the United States.¹⁷⁵ Instead of adopting comprehensive regulation, the United States should only pursue regulatory solutions that promote commercial innovation, which is essential to reducing the high costs of health care. Such limited regulatory solutions—modeled after certain provisions of the GDPR—should focus on providing users with clear notice and consent regarding the privacy policies of applicable companies. Through this approach, the United States will strike a healthy balance between user privacy and commercial innovation.

data-privacy-law.

170. Troiano, *supra* note 1, at 1748.

171. Council Regulation 2016/679, 2016 O.J. (L 119).

172. *General Data Protection Regulation*, WIKIPEDIA, https://en.wikipedia.org/wiki/General_Data_Protection_Regulation (last updated Nov. 23, 2018).

173. *Id.*

174. Derek Hawkins, *The Cybersecurity 202: Why a Privacy Law Like GDPR Would be a Tough Sell in the U.S.*, WASH. POST (May 25, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/25/the-cybersecurity-202-why-a-privacy-law-like-gdpr-would-be-a-tough-sell-in-the-us/5b07038b1b326b492dd07e83/?noredirect=on&utm_term=.0fa3338ce6e6. The GDPR “requires companies that collect data on E.U. citizens to use simple language to explain how they handle it. *Id.* Companies must get explicit consent from consumers before doing anything with their information and allow them to request copies of their data or delete it entirely. *Id.* The law also mandates that companies report data breaches on strict timelines. *Id.* Fines for violations could cost them 4% of their global profits.” *Id.*

175. Berman, *supra* note 166; *see also* Hawkins, *supra* note 174.

Adopting regulation similar in complexity to the GDPR,¹⁷⁶ for example, would likely prove problematic for the United States given the high development and implementation costs required. From an implementation standpoint, a comparable regulation would impose two primary costs on applicable companies—data process reconfiguration and compliance.¹⁷⁷ Research evaluating GDPR preparedness, for example, found that nearly two-thirds of affected companies expect the regulation to “significantly change” their informational workflows and the average company budget necessary to achieve GDPR compliance exceeded nearly \$13 million.¹⁷⁸ A similar study estimated the regulation to collectively cost Fortune 500 companies nearly \$7.8 billion—the majority of which is likely to be recurring—to adequately understand and comply with the new regulation.¹⁷⁹ Such excessive reconfiguration and compliance costs may simply be too high a cost to pay, especially given the stifling effect such regulation could have on innovation. Those in favor of heightened regulations should also be warned that a major incentive for companies in developing innovative software and Internet of Things products is the high margins associated with selling large aggregated datasets that accompany the business model.¹⁸⁰ Regulation that stifles innovation should be especially concerning for the health care industry, which desperately needs innovative solutions to help combat rising costs.¹⁸¹

In addition, regulation with standards as extreme as those of the GDPR would likely present inherent conflicts with America’s constitutional principles and regulatory environment. The opening paragraph of the GDPR, for example, “elevate[s] data privacy into the realm of individual rights,”¹⁸² with a subsequent chapter clarifying

176. *America Should Borrow from Europe’s Data-Privacy Law*, *supra* note 169. Critics argue that the GDPR is simply “too complex and tries to achieve too many things.” *Id.*

177. Will Rinehart, *Should the US Adopt the GDPR*, TECHNOLOGY LIBERATION FRONT (Oct. 1, 2018), <https://techliberation.com/2018/10/01/should-the-us-adopt-the-gdpr/>.

178. *Id.* Another survey found that nearly 88% of companies spent more than \$1 million on GDPR preparations, while 40% spent over \$10 million. *Id.*

179. *Id.*

180. McKinsey analysts “estimate that a retailer embracing big data has the potential to increase its operating margin by more than 60 percent.” James Manyika et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY GLOBAL INST. (Apr. 11, 2012), <https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/big-data-the-next-frontier-for-innovation>; see also Alan Lewis & Dan McKone, *To Get More Value from Your Data, Sell It*, HARV. BUS. REV. (Oct. 21, 2016), <https://hbr.org/2016/10/to-get-more-value-from-your-data-sell-it/>.

181. See Kellogg, *supra* note 15, at 77.

182. Berman, *supra* note 166. The opening paragraph of the GDPR states, “The protection

other fundamental rights surrounding data.¹⁸³ Such rights would likely be considered “out of step with America’s constitutional guarantee of free speech.”¹⁸⁴ Similarly, another section of the GDPR allows only for the processing of personal data “if [the data] fits into one of only six legal basis”—with any other processing deemed illegal by default.¹⁸⁵ Moreover, the regulation creates a regulatory framework that mandates steep penalties for failure to comply (i.e., the greater of €20 million¹⁸⁶ or 4% of the offender’s global revenue).¹⁸⁷ Such monumental fines significantly outweigh even the largest data breach lawsuit settlements in the United States.¹⁸⁸ From a regulatory standpoint, no government agency in America exists or has been granted clear authority to implement such a regulation.¹⁸⁹ In contrast, European Union member states have data privacy authorities to enforce the GDPR.¹⁹⁰ Thus, America, in many ways, maintains “an antiquated policymaking infrastructure” that is more like “a patchwork of controls [with] no unifying principles and no unifying institutions to coordinate policy.”¹⁹¹ Our politically gridlocked government encounters challenge enough when

of natural persons in relation to the processing of personal data is a fundamental human right.” *Id.*; see also Council Regulation, *supra* note 171.

183. Berman, *supra* note 166. The third section of the GDPR entitled, “Rights of data subjects,” outlines the following rights: “the right to access data; the right to correct mistaken data; the right to move data to another platform or provider; the right to restrict or prohibit processing of data; and, most controversially, the right to erasure (sometimes called ‘the right to be forgotten’).” *Id.*; see also Council Regulation, *supra* note 171.

184. *America Should Borrow from Europe’s Data-Privacy Law*, *supra* note 169.

185. Berman, *supra* note 166.

186. *Id.*

187. *Id.* The GDPR effectively mandates that applicable companies “hire a Data Protection Officer, regularly engage in Privacy Impact Assessment, include certain clauses in their contracts with third-parties, partially restrict the transfer of personal data outside the European Union, and provide both a government enforcement mechanism and a private right of action for those who believe they have had their data rights violated. . . . [the regulation] also requires reporting in the case of a data breach, and provides a very short window (72 hours) for companies to make this report.” *Id.*

188. *Id.*

189. *Id.*

190. Hawkins, *supra*, note 174. In America, the closest equivalent to data privacy authorities in European Union member states is likely the FTC, which is considered “the main agency that enforces U.S. privacy policy” though “its powers are thin compared to its European counterparts” and “has little to no oversight over a range of businesses and industries, including airlines, universities, nonprofit organizations and banks.” *Id.* According to William Kovacic—a former general counsel, member, and chair of the FTC during the Obama and Bush administrations—the FTC could try to “use its rulemaking authority to promulgate a set of commands,” but “there’s no public institution in the U.S. that has that breadth of authority, and that’s a big gap.” *Id.*

191. *Id.*

attempting to pass simple legislation—so expecting Congress to approve a regulation as complex as the GDPR seems quite unrealistic, especially when considering inherent conflicts.¹⁹² Further, any such regulation would likely encounter significant resistance from powerful technology lobbyist groups,¹⁹³ arguing that any implemented policy would instantly be outdated.¹⁹⁴ Besides, even if America never adopted a regulation mirroring the GDPR, applicable companies with operations in Europe (or those that serve citizens of the European Union) would still be required to comply with its policies.¹⁹⁵ For these reasons, developing and adopting a comprehensive regulation that mimics the GDPR is a less than ideal solution to the current gap in regulatory protection surrounding personal health data.

Still, a strong case can be made for copying select features of the GDPR that are likely to function effectively in America. One such feature is the GDPR's requirement that companies provide users with clear notice and informed consent about the collection, use, and dissemination of personal information.¹⁹⁶ Though no one wants technology to develop at the snail's pace of government, most Americans still hold strong views about the value of privacy in their everyday lives.¹⁹⁷ And such privacy plays a crucial role in human development by ensuring individuals have "breathing room to engage in the process of . . . self-development," albeit imperfectly.¹⁹⁸ That process becomes especially important when it comes to health. After all, achieving optimal

192. *Id.* "Privacy legislation far less sweeping than the GDPR has stalled over and over in recent years. Legislation to create a federal standard for how companies and agencies report data breaches, for example, has repeatedly dead-ended—even after hackers stole the personal information of 22 million federal workers from the White House Office of Personnel Management in 2014." *Id.*

193. *Id.* "Privacy legislation far less sweeping than the GDPR has stalled over and over in recent years. Legislation to create a federal standard for how companies and agencies report data breaches, for example, has repeatedly dead-ended—even after hackers stole the personal information of 22 million federal workers from the White House Office of Personnel Management in 2014." *Id.*

194. Kellogg, *supra* note 15, at 77.

195. Hawkins, *supra* note 174; *see also* Nick Ismail, *Should the US Adopt GDPR?*, INFORMATION AGE (Nov. 23, 2018), <https://www.information-age.com/us-adopt-gdpr-123469401/>.

196. Berman, *supra* note 166.

197. Madden & Rainie, *supra* note, 109. "[A] majority of Americans believe it is important - often 'very important' - that they be able to maintain privacy and confidentiality in commonplace activities of their lives." *Id.*

198. Sadowski, *supra* note 130.

personal health often takes a lifetime of trial and error. Thus, preserving consumer privacy rights surrounding wearables data serves the public interest.

For example, wearable manufacturers could be required to provide clear notice to users regarding what personal information is being collected,¹⁹⁹ how it will be used,²⁰⁰ and with whom it will be shared.²⁰¹ Though such notice is already commonly presented to users through traditional privacy policies,²⁰² few people actually read such policies due to excessive length and confusing jargon. A recent study, for example, found that only 16% of Internet users consistently read privacy policies of the websites and services with which they share information.²⁰³ Moreover, if all Internet users in the United States read the privacy policy when visiting a website for the first time, each person would expend nearly 244 hours per year—or forty minutes per day.²⁰⁴ Despite these staggering statistics, perhaps the most significant problem with privacy policies is that they attempt to serve widely different functions for multiple parties.²⁰⁵ Companies, for example, use privacy policies to limit liability and demonstrate compliance, but regulators use them for legal enforcement.²⁰⁶ Meanwhile, consumers are often neglected and left relatively uninformed in making decisions about their privacy.²⁰⁷ Since most privacy policies are neither intelligible nor accessible, many drastically limit consumer choice beyond simply using or not using the service.²⁰⁸ For that reason, most users provide their data to companies in exchange for free or reduced-cost services with few limitations, if any, on how the company uses their data.²⁰⁹

199. Edith Ramirez, Chairwoman of the FTC, suggests “the question is not whether consumers should be given a say over unexpected uses of their data; rather, the question is how to provide simplified notice and choice.” Kellogg, *supra* note 15, at 78.

200. Jessica Kitain, *Beware of Wearables: Protecting Privacy in a Data-Collecting World*, 9 DREX. L. REV. ONLINE 1, 26 (2016).

201. *Id.*

202. *Id.*

203. Chris Morran, *1-In-5 Internet Users Always Read Privacy Policies, but That Doesn't Mean They Understand What They're Reading*, CONSUMERIST (Nov. 28, 2012), <https://consumerist.com/2012/11/28/1-in-5-internet-users-always-read-privacy-policies-but-that-doesnt-mean-they-understand-what-theyre-reading/>.

204. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A.J. OF L. & POL'Y 543, 563 (2008).

205. *Nobody Reads Privacy Policies*, *supra* note 126.

206. *Id.*

207. *Id.*

208. *Id.*

209. Berman, *supra* note 166.

In response to these challenges, many are calling for more practical and consumer friendly privacy policies that enable more meaningful choices among users.²¹⁰ Similar to the GDPR, which requires privacy policies to use “clear and plain language” and to be in a “concise, transparent, intelligible and easily accessible form,”²¹¹ companies could be required to provide clearer language.²¹² Such requirements could empower users with more dynamic choices regarding their personal data. A starting point for developing more consumer friendly privacy policies is to make them more relevant and actionable.²¹³ For example, a company could divide an otherwise lengthy privacy policy into smaller subsections to be delivered to users during contextually appropriate times rather than all at once.²¹⁴ To help users process the smaller subsections, companies could incorporate scrollable content, pop-up screens, or large readable text.²¹⁵ Emphasizing the collection of “unexpected or surprising types of data” is another effective way to enhance choice through notice.²¹⁶ Wearable manufacturers could also present users the option of having their geolocation tracked or require explicit approval for each external entity with whom they may share personal data.²¹⁷ Such features could easily be applied to consents as well (e.g., pop-up notifications and click through options).²¹⁸ Additionally, keeping users informed of any changes after initial consent and maintaining accurate records of such—while always allowing users the option of withdrawing consent—is paramount to an effective privacy policy.²¹⁹ Adopting these types of features could transition wearable manufacturers from their archaic all-or-nothing privacy policies²²⁰ to more dynamic contracts that give users real choices.²²¹ Equipping otherwise ignorant users with enhanced knowledge and options would not only increase transparency, but also build trust in the expanding wearables market.

210. *Id.*

211. *Nobody Reads Privacy Policies*, *supra* note 126.

212. Kitain, *supra* note 200, at 27.

213. *Id.*

214. *Id.*

215. *Id.*

216. *Nobody Reads Privacy Policies*, *supra* note 126.

217. Kitain, *supra* note 200, at 27.

218. *Id.*

219. *Id.*

220. *Id.*

221. *Nobody Reads Privacy Policies*, *supra* note 126.

V. CONCLUSION

As society continues to promote and embrace technological advancement, wearables are likely to remain at the heart of data monitoring, despite their apparent drawbacks. Considering the current limits of America's regulatory landscape, however, both commercial and regulatory entities should be thoughtful as they explore potential solutions to the issues surrounding the generation and dissemination of personal health data—particularly data generated by wearables. Government should be especially cautious of comprehensive regulation since its stifling effect on innovation may impede commercial attempts to reduce health care costs and improve population health. Only through the pursuit of limited legislation emphasizing clear notice and consent from users will our country effectively strike a healthy balance between privacy and innovation.

Erika J. Nash