10-1-2016

Apple Watch-ing You: Why Wearable Technology Should be Federally Regulated

Grant Arnow

APPLE WATCH-ING YOU: WHY WEARABLE TECHNOLOGY SHOULD BE FEDERALLY REGULATED

Grant Arnow[*]

I. INTRODUCTION

In 1962, *The Jetsons* introduced a robust vision of the future to American television audiences.[1] The show predicted an interconnected lifestyle, in which intuitive electronics would function to improve peoples' health and happiness.[2] As today's consumer electronics industry expands to offer a multitude of sensor-based and connected devices, apparently "ours is the era of *Novum*," where science fiction becomes science fact.[3]

Indeed, electronic sensors are now ubiquitous in homes, workplaces, and automobiles.[4] Known collectively as the "Internet of Things" (IoT), these networked devices generate unprecedented quantities of detailed information about users' everyday actions, habits, personalities, and preferences.[5] When interpreted by companion software applications, this information helps consumers

* J.D. Candidate, May 2017, Loyola Law School, Los Angeles; B.A. Music, 1999, Miami University. I would like to thank the tireless editorial staff of the *Loyola of Los Angeles Law Review*, including Lilian Walden, Kristin Haule, Michael Lee, Mary Eliza Haney, and Ashley Sarkozi for their hard work and abundant support. My sincere gratitude goes to Professor Karl Manheim for his indispensable guidance, editorial feedback, and encouragement. I am indebted to Michael Kreiner and Elena Grieco, both of whom provided critical, meticulous editing feedback. Finally, I offer my deepest thanks to my family, including my father and mother, my sister, my wife Stephanie, and my sons Remington and Desmond, for their continued patience, love, and inspiration.

1. *See* Matt Novak, *50 Years of the Jetsons: Why the Show Still Matters*, SMITHSONIAN.COM (Sept. 19, 2012), http://www.smithsonianmag.com/history/50-years-of-the-jetsons-why-the-show-still-matters-43459669 ("[T]his little show—for better and for worse—has had a profound impact on the way that Americans think and talk about the future.").

2. *See id.*

3. Joe Concannon, *Connected Home + Wearable Tech = The Jetsons*, DIG. TELEPATHY (July 6, 2015), http://www.dtelepathy.com/blog/inspiration/connected-home-wearable-tech ("[T]he intersection of wearables and connected home technologies . . . is right up there with NASA flying past Pluto.").

4. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 85 (2014).

5. *See id.*

shape lifestyle choices by allowing them to monitor their behavior through previously immeasurable qualities.[6]

As a subset of the IoT, wearable technology allows consumers to monitor and interpret their personal health information by measuring heart rate, stress level, brain activity, respiration, and body temperature, among other data.[7] Users who wear the devices (typically on their wrists) can "track almost any aspect of their health without having to think about it."[8] As such, wearable devices are revolutionizing healthcare by generating real-time "electronic health records," exposing users to personalized feedback regarding everything from blood pressure to oxygen saturation.[9]

Wearable devices also present an easier, more reliable method for healthcare professionals to monitor patients by enhancing consumers' ability to share information with physicians.[10] Put simply, for the healthcare industry, access to patients through wearable devices "could indeed be a significant step in patient engagement and [in] improving population health—two critical success factors driving today's increasingly complex healthcare environment."[11]

Wearable technology, however, also poses significant concerns with regard to consumer privacy and data security.[12] First, wearable devices generate personalized data records, logging unprecedented volumes of personally identifiable health information within networked application servers.[13] The companies creating these

6. *See id.* at 89.

7. *See* Matthew R. Langley, *Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables*, 103 GEO. L.J. 1641, 1642 (2015) ("Consumer wearables present a new way for individuals to communicate sensitive, personal information about themselves.").

8. Luke Villapaz, *CES 2015 Preview: Connected Health and Wearable Tech Will Take Center Stage in 2015*, INT'L BUS. TIMES (Dec. 29, 2014, 5:49 PM), http://www.ibtimes.com/ces-2015-preview-connected-health-wearable-tech-will-take-center-stage-2015-1769180.

9. Vala Afshar & David Peterson, *Wearable Technology: The Coming Revolution in Healthcare*, HUFFINGTON POST (May 4, 2014), http://www.huffingtonpost.com/vala-afshar/wearable-technology-the-c_b_5263547.html (examining wearable technology's impact on the healthcare industry).

10. *See* Langley, *supra* note 7, at 1644 ("Unlike handheld devices, wearable devices can monitor and record physical activity and sensitive health information—such as a user's heart rate, skin temperature, or respiratory rate—in real time.").

11. Afshar, *supra* note 9.

12. *See* Langley, *supra* note 7, at 1642 (examining privacy concerns); *see also* Peppet, *supra* note 4, at 133–34 (evaluating security vulnerabilities).

13. *See* Amber Hunt, *What Wearable Technology Could Mean for Your Privacy*, CINCINNATI.COM (Feb. 12, 2015, 2:29 PM), http://www.cincinnati.com/story/news/2015/02/05/wearable-technology-boom-piques-privacy-concerns/22870621 (examining privacy concerns inherent in wearable technology).

products "can't always ensure [that] the data collected won't end up in unintended hands, or be used for unauthorized purposes."[14] Second, the data generated by wearable devices is of priceless value to marketers, who use it to tailor advertisements to consumers; a form of behavioral advertising.[15] Because wearable technology is new, and evolving rapidly, its innovation eclipses the existing regulatory framework and outpaces the legislative process.

As such, wearable technology should be federally regulated to protect consumer privacy, to secure consumer data, and to foster innovation. Part II of this Note examines the benefits of collecting and interpreting personal health information through the use of wearable devices, and analyzes inherent threats to consumer privacy and data security. Part III evaluates whether users of wearable technology can maintain a reasonable expectation that their personal health information will remain private. Part IV explores why the current federal regulatory scheme fails to sufficiently protect consumer privacy or the security of consumer data collected by wearable devices. Part V offers recommendations for the development of a federal agency to oversee networked information, including the development and implementation of wearable devices. Alternatively, improved user privacy and data security might be accomplished through an enhancement of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Finally, Part VI concludes with an argument that federal regulation of wearable technology will foster innovation, and, ultimately, serve the interests of improving human health.

II. BACKGROUND

Wearable technology comprises a rapidly expanding universe of networked devices that use sensors to track activities and record personal health information.[16] Commonly known as "smart watches," popular wearable devices such as the Apple Watch,[17] Fitbit,[18] and Jawbone Up[19] tap into the "connected self," aggregating

14. *Id.*

15. *See id.*

16. *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 1 (2015), at 1–2, http://jolt.richmond.edu/v21i2/article6.pdf.

17. *See Apple Watch*, APPLE, http://www.apple.com/watch (last visited Dec. 11, 2015).

18. *See* FITBIT, https://www.fitbit.com (last visited Dec. 11, 2015).

19. *See UP by Jawbone*, JAWBONE, https://jawbone.com/up (last visited Dec. 11, 2015).

and transmitting volumes of personal information, including physical activity, sleep patterns, calorie consumption, heart rate, and blood pressure ("biometric data"), as well as geolocational information, to computers and smartphone devices.[20] This personal data is translated and summarized by companion software applications, which purportedly provide tailored feedback to motivate users to engage in healthier, better-informed lifestyles.[21]

Wearable technology's inherent benefits have stimulated an explosive boom in consumers, with sales projected to treble within the next five years.[22] Together with its innovation, however, wearable technology's expanding universe also carries evolving legal implications as to consumer privacy and data security.

A. Wearable Technology's Benefits

Wearable technology is generally recognized for improving consumers' capacity to monitor personal health and fitness information.[23] As wearable devices become more popular, however, epidemiologists also anticipate significant value in analyzing the aggregated health information generated by these devices.[24]

---

20. Nancy F. Butte et al., *Assessing Physical Activity Using Wearable Monitors: Measures of Physical Activity*, MED. & SCI. SPORTS & EXERCISE, Jan. 2012, at S5, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.472.5136&rep=rep1&type=pdf (examining wearable technology's capacity to measure "[d]uration, frequency, and intensity of physical activity," "sleep and awake time," and heart rate); *see also* Robert A. Connor, *Wearable Caloric Intake Monitoring: The Good, the Bad and the Maybe*, WEARABLE TECH WORLD (June 4, 2015), http://www.wearabletechworld.com/topics/wearable-tech/articles/404523-wearable-caloric-intake-monitoring-good-bad-the-maybe.htm (exploring wearable technology's potential to monitor caloric intake); Nina Lincoff, *Wearable Technology: A 'Wristwatch' to Measure Blood Pressure*, HEALTHLINE (June 22, 2013), http://www.healthline.com/health-news/tech-blood-pressure-monitor-in-the-form-of-a-watch-062213 (examining wearable technology's potential to record continuous blood pressure).

21. *See* Thierer, *supra* note 16, at 19 ("As they grow more sophisticated, wearable health devices will help users track, and even diagnose various conditions, and potentially advise a course of action or, more simply, remind users to take medications or contact medical professionals as necessary.").

22. *See* Paul Lamkin, *Wearable Tech Market to Treble in Next Five Years*, FORBES (Oct. 29, 2015, 8:19 AM), http://www.forbes.com/sites/paullamkin/2015/10/29/wearable-tech-market-to-treble-in-next-five-years ("The wearable tech industry will treble inside the next five years—with a whopping 245 million devices expected to ship in 2019 . . . [and] a growth in monetary value of 64 per cent; from $15 billion in 2015 to $25 billion in 2019.").

23. *See* Langley, *supra* note 7, at 1644 ("[M]ost [wearable devices] have a common goal—to recreationally track health and fitness levels.").

24. *See* Drew Schiller, *Wearable Devices: Driving More Value in the Clinical Trial Model*, MHEALTH NEWS (Oct. 29, 2015), http://www.mhealthnews.com/blog/wearable-devices-driving-more-value-clinical-trial-model ("[Wearable devices] could not only benefit researchers during every phase of the clinical trial, but also the participants, as [they] would allow for passive trial adherence and more consistent, higher-resolution data.").

1. Personal Health and Fitness

Wearable devices offer a tailored data stream of personal health information, designed to help consumers understand what potential future impact a lifestyle choice might have on a lifespan. For example, a 2010 study of 123,216 people, published in the *American Journal of Epidemiology*, established that time spent sitting correlated with premature mortality, regardless of total physical activity.[25] Wearable devices illuminate these sedentary habits, and actually motivate consumers to make better lifestyle choices, by, for example, reminding consumers to stand after extended periods of sitting.[26] Furthermore, studies show that consumers tend to rely on devices that actually help to form healthy habits and behaviors as opposed to devices that merely record and report data.[27] Technology experts predict that wearable devices, as an extension of the IoT, may eventually synchronize with supermarket sensors to guide consumer behavior with real-time shopping and health advice.[28]

2. Epidemiological Data Aggregation

The expansion of low-cost wearable health monitors also promises to revolutionize the clinical trials industry. Because wearable devices are increasingly designed for use throughout continuous periods of activity, they generate complete personal health records, more densely nuanced than previous clinical

25. *See* Alpa Patel et al., *Leisure Time Spent Sitting in Relation to Total Mortality in a Prospective Cohort of US Adults*, 172 AM. J. EPIDEMIOLOGY 419, 419 (2010), http://aje.oxfordjournals.org/content/172/4/419.full.pdf+html ("The time spent sitting [greater-than, or equal-to six hours per day] was independently associated with total mortality, regardless of physical activity level.").

26. *See* Mitesh S. Patel et al., *Wearable Devices as Facilitators, Not Drivers, of Health Behavior Change*, 313 J. AM. MED. ASS'N 459, 459 (2015), http://www.telbios.com/wp-content/uploads/2015/01/jvp140141.pdf ("The notion is that by recording and reporting information about behaviors such as physical activity or sleep patterns, these devices can educate and motivate individuals toward better habits and better health.").

27. *See* DAN LEDGER & DANIEL MCCAFFREY, ENDEAVOUR PARTNERS, INSIDE WEARABLES: HOW THE SCIENCE OF HUMAN BEHAVIOR CHANGE OFFERS THE SECRET TO LONG-TERM ENGAGEMENT 5 (2014), http://endeavourpartners.net/assets/Endeavour-Partners-Wearables-White-Paper-20141.pdf ("Products and services that provide utility but fail to have a meaningful impact on users' behaviors and habits—such as an activity tracker that provides data but doesn't inspire action—end up failing in the market. Users quickly abandon wearables that don't help them make positive changes. Devices that offer functionality to help the wearer change their habits also promote sustained behavior change and lead to long-term health.").

28. *See* Roy Wallack, *Wearable Technology Catapulting Health and Fitness into Future*, L.A. TIMES (Jan. 23, 2015), http://www.latimes.com/health/la-he-future-wearables-20150124-column.html (predicting the impact wearable technology will have on health and fitness).

measurements would allow.[29] For example, while researchers previously struggled to motivate clinical participants to travel to designated testing sites or to manually report accurate data, the use of wearable devices "enable[s] consumers to passively track their health data 24/7, including when they are sleeping, which ensures the accuracy and timeliness of the information."[30] Furthermore, networked clinical trials allow participants to upload personalized biomedical records to clinical databases with greater ease, reducing both the time in which the information can be analyzed and the cost of doing so.[31] Critically, individualized data's rapid aggregation within regional and global clinical trials creates powerful potential to generate data sets that aid in identifying medical subgroups.[32]

Rather than diagnosing patients with generalized conditions like diabetes or asthma, it may soon be possible to identify "phenotypically distinct [patient] subgroups, in which the underlying cause of a disease might be molecularly distinct."[33]

Wearable technology is therefore enormously valuable for patient profiling and "precision medicine," which evaluates variability in genes, environments, and lifestyles for each person.[34] As articulated recently by President Obama, precision medicine promises to improve health and revolutionize disease treatment by

29. *See* Bradford W. Hesse et al., *From Big Data to Knowledge in the Social Sciences*, 659 ANNALS AM. ACAD. POL. & SOC. SCI. 16, 27 (2015) ("The new mobile sensing technologies that are becoming ubiquitous as part of the 'wearable device' revolution can provide the capability to collect rapidly recorded behavioral data, often unobtrusively." (citations omitted)).

30. *See* Schiller, *supra* note 24.

31. *See* Hesse et al., *supra* note 29, at 26–27 ("The consumer-facing, and often provocative, gene sequencing company 23andMe caught the attention of biomedical scientists when it demonstrated how it was possible to replicate the findings of a large NIH-funded trial in less than one-sixth of the time and a fraction of the cost for the original study." (citation omitted)).

32. *See* David Shaywitz, *Wearables as Tools for Precision Medicine: Promise in Search of Evidence*, FORBES (Feb. 7, 2015, 8:43 PM), http://www.forbes.com/sites/davidshaywitz/2015/02/07/wearables-as-tools-for-precision-medicine-a-promise-in-search-of-evidence ("The theory is compelling—with the opportunity to monitor patients more comprehensively, and track patients in a fashion that more closely follows the contours of their lives, it should be possible to derive a more complete dataset that enables useful subgroups to be identified.").

33. *Id.*

34. *Fact Sheet: President Obama's Precision Medicine Initiative*, THE WHITE HOUSE (Jan. 30, 2015), https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative [hereinafter *PMI Fact Sheet*]; *see also* David Shaywitz, *Revisiting the Central Dogma of Precision Medicine*, FORBES (Apr. 15, 2015, 9:48 PM), http://www.forbes.com/sites/davidshaywitz/2015/04/15/revisiting-the-central-dogma-of-precision-medicine ("The core premise . . . of precision medicine . . . is that the integration of genetic information . . . and rich dynamic phenotypic information will enable sophisticated patient segmentation, revealing biologically distinct subgroups and pointing the way to precisely targeted treatments.").

accelerating biomedical discoveries, providing clinicians with new tools, knowledge, and therapies to select effective treatments for individual patients.[35]

B. Concerns About Wearable Technology

Wearable technology's myriad benefits, however, are counterbalanced by the fact that the technology exposes consumers to novel, evolving threats to privacy and data security. Many wearable devices maintain continuous network connections that threaten to open a largely unregulated door into users' private lives.[36] "The massive amount of data these new wearable devices stand to collect, the sensitive nature of the content, and the uncertainty about how the information can be used have all raised concerns that consumers are being lured into uncharted territory that will compromise their privacy."[37] Making matters worse, wearable devices often obscure the collected personal health information within an "opaque bubble" of interconnected networks, distorting consumer awareness and making permanent deletion difficult (if not impossible).[38]

These evolving concerns have already prompted regulation in other parts of the world. For example, in June 2014, the United Kingdom's Information Commissioner's Office (ICO) determined that the collection and processing of personal information performed by wearable devices must adhere to the U.K. Data Protection Act's standards.[39] While that Act currently applies a narrow exemption to devices collecting information exclusively for personal purposes, the

35. *PMI Fact Sheet*, *supra* note 34 (explaining President Obama's Precision Medicine Initiative).

36. *See* Hayley Tsukayama, *Wearable Tech Such as Google Glass, Galaxy Gear Raises Alarms for Privacy Advocates*, WASH. POST (Sept. 30, 2013), https://www.washingtonpost.com/business/technology/wearable-technology-raise-privacy-concerns/2013/09/30/0a81a960-2493-11e3-ad0d-b7c8d2a594b9_story.html (examining threats to privacy attendant to the development of wearable technology).

37. *Id.*

38. *See* Teena Maddox, *The Dark Side of Wearables: How They're Secretly Jeopardizing Your Security and Privacy*, TECHREPUBLIC (Oct. 7, 2015), http://www.techrepublic.com/article/the-dark-side-of-wearables-how-theyre-secretly-jeopardizing-your-security-and-privacy ("There is an opaque bubble around all of this data . . . [and] a complexity around the deletion of data.").

39. *See* Andrew Paterson, *Wearable Technology—the Future of Privacy*, INFO. COMM'R'S OFF. BLOG (June 26, 2014), https://iconewsblog.wordpress.com/2014/06/26/wearable-technology-the-future-of-privacy ("[L]ike any new technology, wearables must operate in compliance with the law. In the UK, this means making sure that these devices operate in line with the requirements of the UK Data Protection Act.").

ICO warned that any other use falls within the act's purview.[40]

1. Wearable Devices Compromise Consumer Privacy

According to the Pew Research Center ("Pew"), a majority of Americans have "a pervasive sense that they are under surveillance," and "few feel they have a great deal of control over the data that is collected about them and how it is used."[41] Furthermore, most lack confidence that online activity, which is tracked and maintained by advertisers, social media websites, government agencies, credit card companies, and search engine providers, will remain private.[42] These concerns are well founded, considering that nearly every major retailer utilizes a "predictive analytics" department to leverage personalized marketing through interpreting individualized consumer behavior.[43]

As consumers search, browse, and shop, their historical behavior is logged within growing relational databases. Much of this information—often referred to as "big data"—is collected without consumer awareness and is sold for a variety of commercial purposes.[44] Big data is valuable to brands and advertisers because it makes information about consumer behavior transparent and usable at a high frequency.[45] Nuanced analytics allow for narrow customer segmentation, precise tailoring of products and services, and improved strategic decision-making.[46] Data mining has become so invasive that the Federal Trade Commission (FTC) recently urged lawmakers to push for transparency and accountability among

40. *See id.*

41. Mary Madden & Lee Raine, *Americans' Attitudes About Privacy, Security and Surveillance*, PEW RES. CTR. (May 20, 2015), at 3, http://www.pewinternet.org/files/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf.

42. Id. at 6–7.

43. *See* Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (examining Target's utilization of big data in strategic advertising and predictive consumer strategy).

44. *See* Lois Beckett, *Big Data Brokers: They Know Everything About You and Sell It to the Highest Bidder*, GIZMODO (Mar. 18, 2013, 10:11 AM), http://gizmodo.com/5991070/big-data-brokers-they-know-everything-about-you-and-sell-it-to-the-highest-bidder ("[Data brokers] sell information about whether you're pregnant or divorced or trying to lose weight, about how rich you are and what kinds of cars you have.").

45. *See* James Manyika, et al., *Big Data: The Next Frontier for Innovation, Competition, and Productivity*, MCKINSEY GLOBAL INST. (June 2011), at 5, http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Big%20Data/MGI_big_data_full_report.ashx.

46. *See id.*

entities that buy and sell personalized data.[47]

But wearable technology's explosive popularity is causing even greater concern among privacy advocates, and for good reason. Wearable technology creates a personalized data profile, recording continuous logs of consumer activity levels through biomedical feedback. This data—which provides priceless insight to marketers, advertisers, retailers, insurers, employers, financial service providers, and social contacts—is stored within vulnerable network systems, the security of which is largely, if not entirely, unregulated.[48]

What results is arguably a "perfect privacy storm": (1) consumers are generally clueless about the range of information that wearable devices record; (2) the data is stored in permanent record, typically across labyrinths of interconnected networks, which utilize insufficient security protocols; and (3) the market for collecting and selling the data is ever booming, offering increasing value for data brokers and hackers alike. Because many wearable devices cultivate and upload personal health information, they represent a significant threat to consumer privacy

2. Manufacturers Fail to Secure the Data Collected by Wearable Devices

As wearable devices become ubiquitous, security experts say that the companies creating these products "can't always ensure [that] the data collected won't end up in unintended hands, or be used for unauthorized purposes."[49] For example, Symantec Corporation, a technology security firm headquartered in California, recently analyzed a variety of wearable activity-tracking devices and found that all of them were vulnerable to location-tracking.[50]

---

47. *See Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N (May 2014), at viii, https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may2014/140527databrokerreport.pdf ("With respect to data brokers that sell marketing products, the Commission recommends that Congress consider legislation requiring data brokers to provide consumers access to their data, including sensitive data held about them, at a reasonable level of detail, and the ability to opt out of having it shared for marketing purposes.").

48. *See* Peppet, *supra* note 4, at 136 ("Data security in the United States is generally regulated through one of two mechanisms: FTC enforcement or state data breach notification laws. Neither is clearly applicable to breaches of [IoT] data. Put differently, if your biometric data were stolen from a company's servers, it is contestable whether any state or federal regulator would have the authority to respond.").

49. Hunt, *supra* note 13.

50. *See How Safe Is Your Quantified Self? Tracking, Monitoring and Wearable Tech*, SYMANTEC OFFICIAL BLOG (July 30, 2014), http://www.symantec.com/connect/blogs/how-safe

Symantec also identified vulnerabilities in the storage and management of personal data, and found that many of the devices were transmitting passwords in clear, unencrypted text.[51] "As the amount of data collected by [these] enterprises continues to grow at a rate of 40 percent to 60 percent per year, IT teams face new challenges in securely managing the vast amounts of information under their watch."[52] And because personal health information has a high black-market value,[53] acquiring or intercepting the data collected by wearable devices is an increasingly enticing opportunity for hackers.

But despite these threats, many businesses still fail to implement adequate data security. Such deficient systems have resulted in an alarming number of recent high-profile security breaches, including Anthem, Inc., and UCLA Health.[54]

III. CAN WEARABLE DEVICE USERS MAINTAIN REASONABLE EXPECTATIONS OF PRIVACY?

As wearable technology dramatically expands the universe of data that consumers share online, the question arises whether traditional notions of privacy still apply. Social networking has conditioned users to share private information liberally. "Facebook alone has more than one billion users, and the average Facebook user shares ninety pieces of information each month."[55] In light of the resulting benefits, many consumers have grown accustomed to sharing such personal information through social networks on a daily

-your-quantified-self-tracking-monitoring-and-wearable-tech.

51. *See id.* ("The transmission of credentials in clear text is especially troubling given that large numbers of people have a propensity to reuse login credentials at multiple sites. Due to reuse, login details stolen from one service could potentially be used to gain access to more sensitive services such as email accounts or online shopping accounts.").

52. *See* Natasha Baker, *Are Your Systems Ready for the Big Data Explosion? 3 Key Database Strategy Tips*, FORBES (Mar. 3, 2015, 11:39 AM), http://www.forbes.com/sites/centurylink/2015/03/13/are-your-systems-ready-for-the-big-data-explosion-3-key-database-strategy-tips.

53. *See* Caroline Humer & Jim Finkle, *Your Medical Record Is Worth More to Hackers Than Your Credit Card*, REUTERS (Sept. 24, 2014, 2:24 PM), http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 ("Your medical information is worth 10 times more than your credit card number on the black market.").

54. *See* Chad Terhune, *UCLA Health System Data Breach Affects 4.5 Million Patients*, L.A. TIMES (July 17, 2015, 5:51 PM), http://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html.

55. Lisa A. Schmidt, *Social Networking and the Fourth Amendment: Location Tracking on Facebook, Twitter, and Foursquare*, 22 CORNELL J.L. & PUB. POL'Y 515, 517 (2012).

basis.[56]

Predictably, teenagers share personal information through online platforms in an even greater volume.[57] According to Pew, eighty-four percent of surveyed teenagers reported that they shared personal interests through social media.[58] Most reported sharing their real name, birthdate, hometown, and the school they attend, with 91 percent having posted a photo of himself or herself.[59] Teens share information through social networks freely and unabashedly, causing some adults to speculate that youth eschew privacy in order to participate in social media.[60] Yet, according to Pew, most teenagers choose to use privacy settings for Facebook, suggesting that they maintain a general expectation that the information they share will remain within some closed universe of relationships.[61]

However, while major social networks allow users to customize their privacy settings to determine the scope of their voluntary posts, many networks (including Facebook, Twitter, and Foursquare) also continuously track geolocational data whenever a user is logged in.[62] Nearly ten years after Apple's introduction of the iPhone,[63] a majority of consumers access and share data with social networks through mobile devices,[64] with many users remaining logged in for extended periods of time.[65] As a result, many consumers unwittingly transmit personal geolocational data from their mobile devices to

56. *See id.* ("The average Facebook user shares ninety pieces of information each month.").

57. *See generally* Amanda Lenhart et al., *Teens, Social Media & Technology Overview 2015*, PEW RES. CTR. (Apr. 9, 2015), at 2, http://www.pewinternet.org/files/2015/04/PI_TeensandTech_Update2015_0409151.pdf ("Aided by the convenience and constant access provided by mobile devices, especially smartphones, 92% of teens report going online daily—including 24% who say they go online 'almost constantly.'").

58. *See* Mary Madden, et al., *Teens, Social Media, and Privacy*, PEW RES. CTR. (May 21, 2013), at 33, www.pewinternet.org/files/2013/05/PIP_TeensSocialMediaandPrivacy_PDF.pdf.

59. *See id.* at 30.

60. Danah Boyd, *The Truth About Teens and Privacy*, BACKCHANNEL (Dec. 23, 2014), https://medium.com/backchannel/the-truth-about-teens-and-privacy-988aee14a203#.q2o1i7u0d; *see also* Emily Nussbaum, *Say Everything*, N.Y. MAG. (Feb. 12, 2007), at 2, http://nymag.com/news/features/27341 ("Kids today. They have no sense of shame. They have no sense of privacy. They are show-offs, fame whores, pornographic little loons who post their diaries, their phone numbers, their stupid poetry—for God's sake, their dirty photos!—online.").

61. *See* Madden et al., *supra* note 58, at 7.

62. *See* Schmidt, *supra* note 55, at 517.

63. *See Apple Reinvents the Phone with iPhone*, APPLE (Jan. 7, 2007), http://www.apple.com/pr/library/2007/01/09Apple-Reinvents-the-Phone-with-iPhone.html.

64. *See* Ray Pun, *Adobe 2013 Mobile Consumer Survey: 71% of People Use Mobile to Access Social Media*, ADOBE DIG. MKTG. BLOG (July 25, 2013), http://blogs.adobe.com/digitalmarketing/mobile/adobe-2013-mobile-consumer-survey-71-of-people-use-mobile-to-access-social-media.

65. *See* Schmidt, *supra* note 55, at 517.

social networks and other application services.[66]

Because social networks can (and do) covertly track consumers' behavior, the mere use of social media might necessarily involve a surrendering of privacy, in spite of any "privacy settings" a service offers. On the other hand, because many users are unaware of the degree to which social networks observe their daily activities, or prohibit them from mastering privacy controls, perhaps consumers have yet to fully comprehend the extent to which they must relinquish their private data in order to use these services. As wearable technology expands to pair biometric data with social networking,[67] one wonders if wearable device consumers have lost any expectation of privacy in their personal health information.

A. The Fourth Amendment

The Fourth Amendment to the U.S. Constitution confers the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[68] "According to the Supreme Court, the Fourth Amendment regulates government conduct that violates an individual's reasonable expectation of privacy."[69] As such, Fourth Amendment precedent can serve as a device to evaluate whether consumers can maintain a reasonable expectation that the personal data collected by wearable devices will remain private.[70]

Justice Harlan's concurring opinion in *Katz v. United States*[71] has come to govern the standard for what qualifies as a search under the Fourth Amendment.[72] Justice Harlan argued that "an enclosed telephone booth [i]s an area where, like a home, and unlike a field, a person has a constitutionally protected *reasonable expectation of privacy*," and "electronic as well as physical intrusion into a place

66. *See* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), https://www.ftc.gov/sites/default/files/documents /reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade -commission-staff-report/130201mobileprivacyreport.pdf ("[M]obile devices can reveal precise information about a user's location that could be used to build detailed profiles of consumer movements over time and in ways not anticipated by consumers.").

67. *See Guest Post, First Biometric Social Network*, NEUROGADGET (June 17, 2015), http:// neurogadget.com/2015/06/17/first-biometric-social-network/11417.

68. U.S. CONST. amend. IV.

69. Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504 (2007) (citing Smith v. Maryland, 442 U.S. 735, 740 (1979) (internal citation omitted)).

70. *See* Schmidt, *supra* note 55, at 517.

71. 389 U.S. 347, 360 (1967).

72. *See* Schmidt, *supra* note 55, at 517.

that is in this sense private may constitute a violation of the Fourth Amendment."[73]

Courts have held that social media users do not have reasonable expectations of the privacy of their social network posts.[74] "Because information that an individual shares through social networking [websites] like Facebook may be copied and disseminated by another, the expectation that such information is private, in the traditional sense of the word, is not a reasonable one."[75] Furthermore, when a person creates a social media account and agrees to the "terms of service" set out by the provider, they consent to the fact that "[their] personal information [will] be shared with others, notwithstanding [their] privacy settings. Indeed, that is the very nature and purpose of these social networking sites, [or] else they would cease to exist."[76]

But traditional notions of a reasonable expectation of privacy may still exist as to data that consumers inadvertently or unknowingly share with social networks, including the automatic geolocational data generated by consumers' mobile devices.

In *United States v. Jones*,[77] the Supreme Court declined to perform a *Katz* analysis in a case involving the surreptitious placement of a GPS device on a suspect's vehicle.[78] The Court held that, because the government's placement of the device amounted to a "classic trespassory search," it was unnecessary for the Court to engage in a "reasonable expectation" inquiry.[79] In his concurring opinion, Justice Alito argued that *Katz* should control, but noted that the *Katz* test "is not without its own difficulties."[80] In evaluating whether the Fourth Amendment might extend any protection to new

73. *Katz*, 389 U.S. at 360–61 (emphasis added) (citations omitted).

74. *See* Nucci v. Target Corp., 162 So. 3d 146, 153–54 (Fla. Dist. Ct. App. 2015) ("[T]he photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy settings that the user may have established."); *see also* Largent v. Reed, No. 2009-1823, 2011 Pa. Dist. & Cnty. Dec. LEXIS 612, at *12 (Pa. C.P. Nov. 8, 2011) ("When a user communicates on Facebook, her posts may be shared with strangers. And making a Facebook page 'private' does not shield it from discovery. This is so because . . . even 'private' Facebook posts are shared with others." (citations omitted)); Romano v. Steelcase Inc., 30 Misc. 3d 426, 434 (N.Y. Sup. Ct. 2010) ("Indeed, as neither Facebook nor MySpace guarantee complete privacy, plaintiff has no legitimate reasonable expectation of privacy.").

75. *Nucci*, 162 So. 3d at 154 (citations omitted) (internal quotation marks omitted).

76. *Romano*, 30 Misc. 3d at 434.

77. 132 S. Ct. 945 (2012).

78. *See id.* at 953–54.

79. *See id.* at 954.

80. *Id.* at 962 (Alito, J., concurring).

technology, Justice Alito observed that

> [d]ramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable. On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions.[81]

Justice Alito concluded that because

> cell phones and other wireless devices now permit wireless carriers to track and record the location of users . . . [and because] phone-location-tracking services are offered as "social" tools . . . the availability and use of these *and other new devices* will continue to shape the average person's expectations about the privacy of his or her daily movements.[82]

Wearable technology's recent (and explosive) popularity unquestionably constitutes a dramatic change in the consumer electronics industry. As technology brands introduce or enhance wearable devices with new functionality, consumers face rapidly shifting privacy implications. Because many wearable devices automatically generate and transmit personal health information, however, their use creates a threat to privacy broader than that which courts have previously evaluated.[83] In fact, the court in *Nucci v. Target Corp.*[84] distinguished a reasonable person's strong privacy interest in his or her medical records from a comparatively weak privacy interest in photographs posted on social networks.[85]

---

81. *Id.* (citations omitted).

82. *Id.* at 963 (emphasis added).

83. The generation and transmission of personal health information extends well beyond the voluntary social media posts analyzed in *Nucci*, *Largent*, and *Romano*. *See* Nucci v. Target Corp., 162 So. 3d 146, 153–54 (Fla. Dist. Ct. App. 2015); Largent v. Reed, 2011 Pa. Dist. & Cnty. Dec. LEXIS 612, at *12–13 (Pa. C.P. Nov. 8, 2011) (internal citations omitted); Romano v. Steelcase, Inc., 30 Misc. 3d 426, 434.

84. *Nucci*, 162 So. 3d at 154.

85. *Id.* ("Such posted photographs are unlike medical records or communications with one's attorney, where disclosure is confined to narrow, confidential relationships.").

The advent of wearable technology represents a significant expansion in the kind of personal information consumers inadvertently share online. The health information collected and transmitted by wearable devices has traditionally been regarded as within the scope that a reasonable person would expect to remain private. As such, courts should utilize *Katz* to independently evaluate whether the Fourth Amendment applies to the personal health data generated and transmitted through the use of wearable technology.[86]

IV. ALLOWING THE FOX TO GUARD THE HENHOUSE: WHY CURRENT FEDERAL REGULATIONS FAIL TO PROTECT WEARABLE DEVICE USERS' PRIVACY AND DATA SECURITY

Despite an increasing number of high-profile network hacks—including, according to the Department of Health and Human Services, more than 1,100 breaches of organizations handling protected health information[87]—the collection and use of personal data in the United States is not yet regulated by a comprehensive federal scheme.[88] Instead, the United States has "a patchwork system" of narrow federal statutes and antiquated agency guidelines that sometimes overlap, dovetail, or contradict state laws and regulations.[89]

The government's sluggish approach to updating federal privacy and data security policies has caused concern among other nations. For example, on October 6, 2015, the European Court of Justice invalidated the European Union ("EU") Data Protection Commission's U.S. Safe Harbor Decision, ending a fifteen-year practice permitting U.S. companies to self-certify compliance with European privacy standards.[90] Now, to legally receive exports of

86. *See Katz*, 389 U.S. at 361.

87. *See* Andrea Peterson, *2015 Is Already the Year of the Health-Care Hack—and It's Only Going to Get Worse*, WASH. POST (Mar. 20, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/03/20/2015-is-already-the-year-of-the-health-care-hack-and-its-only-going-to-get-worse.

88. *See* Ieuan Jolly, *Data Protection in the United States: Overview*, PRAC. L. (July 1, 2015), http://us.practicallaw.com/6-502-0467#null.

89. *See id.*; *see also* Ricardo Alonoso-Zaldivar, *Federal Health Privacy Law Leaves Consumer Data Vulnerable to Hackers*, THE REG. GUARD (Feb. 6, 2015), http://registerguard.com/rg/news/32744498-76/federal-health-privacy-law-leaves-consumer-data-vulnerable-to-hackers.html.csp ("Insurers aren't required to encrypt consumers' data under a 1990s federal law that remains the foundation for healthcare privacy in the Internet age—an omission that seems striking in light of the major cyberattack against Anthem . . . .").

90. *See* Kyle Wood et al., *U.S. No Longer Safe Harbor for European Data*, NAT'L L. REV. (Oct. 19, 2015), http://www.natlawreview.com/article/us-no-longer-safe-harbor-european-data

personal data from Europe, U.S. companies must comply with the EU's tighter approach to data privacy and protection, forcing a "fundamental restructuring of the way many companies currently collect, store and transfer personal data."[91]

Put simply, the legislative process cannot keep pace with technological innovation, and federal agencies are slow to adapt to new technologies. Accordingly, the United States currently offers an insufficient regulatory framework to protect consumers' privacy as to wearable technology or to secure the personal health information cultivated by such devices. "At least for the moment, there is no clear legislative or judicial framework that squarely addresses all of the concerns raised by the development of these devices."[92] Consequently, when consumers use wearable devices to record and upload personal health information, their data remains perpetually vulnerable, not only to hackers and cybercriminals, but also to advertisers, insurers, employers, and ex-lovers alike.

A. Popular Wearable Devices Are Not Subject to Federal Oversight

No federal agency seems inclined to take charge of regulating popular wearable devices. The Food and Drug Administration (FDA) is the only agency to even address the issue, indicating with a recent draft guidance that the agency will not vigorously regulate wearable devices as long as the devices generally encourage healthy habits.[93] According to Bakul Patel, the FDA's Associate Director for Digital Health, the agency plans to take a "very light touch, an almost hands-off approach" to wearable devices that are designed to "motivate a

("The European Union Data Protection Directive forbids the transfer of personal data to a country outside the European Economic Area ('EEA') unless that country has adequate data protection measures in place.").

91. *See id.*

92. Karen H. Bromberg & Duane C. Cranston, *Wearable Technology: Taking Privacy Issues to Heart*, N.Y.L.J., Mar. 2, 2015, http://www.newyorklawjournal.com/id=1202719019470/Wearable-Technology-Taking-Privacy-Issues-to-Heart.

93. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., FDA, GENERAL WELLNESS: POLICY FOR LOW RISK DEVICES, DRAFT GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2015), at 2, http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM429674.pdf?source=govdelivery&utm_medium=email&utm_source=govdelivery [hereinafter *FDA Draft Guidance*]; *see also* Colin Lecher, *The FDA Doesn't Want to Regulate Wearables, and Device Makers Want to Keep It That Way*, THE VERGE (June 24, 2015, 2:07 PM), http://www.theverge.com/2015/6/24/8836049/fda-regulation-health-trackers-wearables-fitbit ("The [FDA draft] guidance effectively suggests the agency won't vigorously regulate devices as long as they're not harmful and generally encourage healthy habits.").

person to stay healthy."[94] This approach ostensibly allows technology manufacturers to innovate without aggressive federal oversight.[95]

Furthermore, the FDA intends to exercise only discretionary enforcement of "[m]obile apps that allow a user to[] collect, log, track and trend data, such as blood glucose, blood pressure, heart rate, [or] weight . . . from a device to eventually share with a healthcare provider, or upload . . . to an online (cloud) database, [or a] personal or electronic health record."[96]

And technology manufacturers—eager to dissuade the FDA from regulating popular wearable devices—are pushing the agency to make its forbearance more explicit.[97] For example, Samsung Electronics America ("Samsung"), commenting in response to the FDA's draft guidance, recently urged the Agency to spare wearable devices that track blood pressure and blood glucose data from regulatory oversight.[98]

But, according to the FDA's Mobile Medical Applications Guidance, consumer mobile applications (and, presumably, wearable devices) become subject to federal regulations by performing sophisticated, patient-specific analysis, providing personalized diagnoses, or recommending treatment options.[99] This creates a dissonance with the Agency's "hands off" approach to wearable devices, because as manufacturers push for decreased federal oversight, they simultaneously enhance the platforms wearable devices use to monitor and interpret biometric data.[100] For example,

---

94. Adam Satariano, *FDA 'Taking a Very Light Touch' Regulating the Apple Watch*, BLOOMBERG (Mar. 30, 2015), http://www.bloomberg.com/news/articles/2015-03-30/fda-taking-a-very-light-touch-on-regulating-the-apple-watch.

95. *See id.*

96. U.S. DEP'T OF HEALTH & HUM. SERVS., FDA, MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 26 (2015), http://www.fda.gov/downloads/MedicalDevices/%20.%20.%20./UCM263366.pdf [hereinafter *FDA Guidance*].

97. Lecher, *supra* note 93.

98. *See* Letter from John Godfrey, Senior Vice President, Pub. Policy, Samsung Elecs. Am., Inc., to Div. of Dockets Mgmt. (HFA-305) (Apr. 20, 2014), at 2–3, http://www.regulations.gov/contentStreamer?documentId=FDA-2014-N0390014&attachmentNumber=1&disposition=attachment&contentType=pdf.

99. *FDA Guidance*, *supra* note 96, at 15.

100. *See* Thomas Flanagan, *Samsung Bio-Processor Makes Big Stride in mHealth Wearables*, RETHINK TECH. RES. (Jan. 8, 2016), http://rethink-iot.com/2016/01/08/samsung-bio-processor-makes-big-stride-in-mhealth-wearables ("Samsung wants to take its Bio-Processor to the next level for the health-conscious consumer by measuring body fat, skeletal muscle mass, heart rate, skin temperature, and stress level (sweatiness).").

Samsung's new "Bio-Processor" chip has the potential to perform diagnostic testing in the same manner offered by medical laboratories.[101] Soon, wearable technology may approximate traditional doctor-patient relationships, all without any attendant regulatory scheme.[102]

The resulting friction between existing regulations and wearable technology's rapid evolution has created an expanding gray area, wherein manufacturers and software developers cannot clearly understand where "personal fitness trackers" end and "personal medical devices" begin. Moreover, the FDA appears unaware of wearable technology's expanding role as a bridge between doctors and patients during "a time when healthcare and consumer technology are blending."[103]

B. Federal Recommendations Fail to Motivate Businesses to Employ Effective Data Security

Despite acknowledging that cybercriminals pose a serious threat to consumers,[104] the federal government has not yet required businesses to employ standardized cybersecurity measures to protect consumer privacy. Instead, federal agencies propagate toothless recommendations to educate businesses on "best practice" data security strategies. For example, in the FTC's recent report on the IoT, the agency recommended a series of steps that businesses could use to protect consumers' privacy and enhance data security.[105]

101. Dava Stewart, *Samsung's New All-in-One Bio-Processor Chip Launches Amid Controversy Among Physicians and Medical Laboratory Professionals over the True Value of Wearable Health Monitoring Devices*, DARK DAILY (Feb. 12, 2016), http://www.darkdaily.com/samsungs-new-all-in-one-bio-processor-chip-launches-amid-controversy-among-physicians-and-medical-laboratory-professionals-over-the-true-value-of-wearable-health-monitoring-devices-0512#axzz40562Jxmv.

102. *See generally* MED. BD. OF CAL., GUIDE TO THE LAWS GOVERNING THE PRACTICE OF MEDICINE (7th ed. 2013), http://www.mbc.ca.gov/about_us/laws/laws_guide.pdf ("This publication is a reference source on the federal and state laws and additional information which govern [physician] medical practice.").

103. Satariano, *supra* note 94.

104. *See* Press Release, Office of the Press Secretary, Remarks by the President at the Federal Trade Commission (Jan. 12, 2015), https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission ("When these cyber criminals start racking up charges on your card, it can destroy your credit rating. It can turn your life upside down.").

105. *See* FED. TRADE COMM'N, THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127iotrpt.pdf [hereinafter *FTC IoT Report*]; Press Release, Fed. Trade Comm'n, FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks (Jan. 27, 2015), https://www.ftc.gov/news-events/press-releases/2015/01/ftc

These recommendations, however, do not carry the force of law.[106] As a consequence, businesses are free to prioritize cybersecurity as they see fit, and use minimal methods if they choose to.[107]

And in spite of the FTC's recommendations, many businesses still fail to implement adequate data security policies. As an initial matter, many businesses (including the federal government)[108] tend to overlook seemingly mundane security measures such as changing passwords and updating anti-virus software during the normal course of business.[109]

Furthermore, comprehensive cybersecurity measures are expensive, and thus, entities tend to dither in determining what level of protection to employ.[110] And because the FTC's recommendations do not carry the force of law, businesses are free to apply a cost-benefit analysis to determine their preferred strategy.[111] As such, businesses need only engage the minimal measures to protect consumer data as will be deemed "reasonable" in the aftermath of a

---

-report-internet-things-urges-companies-adopt-best-practices [hereinafter *FTC Press Release*].

106. *See FTC Press Release*, *supra* note 105 ("We believe that by adopting the *best practices* we've laid out, businesses will be better able to provide consumers the protections they want and allow the benefits of the [IoT] to be fully realized." (quoting FTC Chairwoman Edith Ramirez) (emphasis added)).

107. *See FTC IoT Report*, *supra* note 105, at 28 ("Of course, what constitutes reasonable security for a given device will depend on a number of factors, including the amount and sensitivity of data collected, the sensitivity of the device's functionality, and the costs of remedying the security vulnerabilities.").

108. *See* Craig Timberg & Lisa Rein, *Senate Cybersecurity Report Finds Agencies Often Fail to Take Basic Preventative Measures*, WASH. POST (Feb. 4, 2014), www.washingtonpost.com /business/technology/senate-cybersecurity-report-finds-agencies-often-fail-to-take -basicpreventivemeasures/2014/02/03/493390c2-8ab6-11e3-833c-33098f9e5267_story.html ("A common password on federal systems . . . is 'password.'").

109. *See* Constance Gustke, *No Business Too Small to Be Hacked*, N.Y. TIMES (Jan. 13, 2016), http://www.nytimes.com/2016/01/14/business/smallbusiness/no-business-too-small-to-be-hacked.
html ("Among the simpler precautions small businesses and consumers alike can take is to create strong passwords . . . [but] it is stunning how many people and small businesses fail to heed the advice.").

110. *See* Danny Yadron, *Companies Wrestle with the Cost of Cybersecurity*, WALL ST. J. (Feb. 25, 2014, 11:24 PM), http://www.wsj.com/articles
/SB10001424052702304834704579403421539734550 ("Companies wrestle daily with the question of how much security is enough.").

111. *See* FED. TRADE COMM'N, DISSENTING STATEMENT OF COMMISSIONER JOSHUA D. WRIGHT, ISSUANCE OF THE INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD STAFF REPORT 1 n.1 (Jan. 27, 2015), https://www.ftc.gov/system/files/documents/public _statements/620701/150127iotjdwstmt.pdf [hereinafter Wright Dissenting Statement] ("Where an agency's recommendations regarding best practices are not supported by cost-benefit analysis, firms may respond by adopting practices or engaging in expenditures that make consumers worse off.").

major hack.[112]

Because wearable devices expose consumers to novel, evolving threats to privacy, the federal government should hold manufacturers and application developers to a higher cybersecurity standard. But because federal recommendations fail to motivate businesses to prioritize sufficient cybersecurity, consumer privacy remains perpetually at risk.

C. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") establishes federal standards to regulate the types of uses and disclosures of personally identifiable health information made by "covered entities," including: (1) health plans, (2) healthcare clearinghouses, (3) healthcare providers who conduct certain transactions electronically, and (4) business associates of covered entities.[113] The HIPAA Security Rule establishes national standards for the security of electronic protected health information, to be implemented by these "covered entities."[114] Because wearable technology allows consumers to monitor and interpret their personal health information, HIPAA is currently in the best position to protect the biometric data cultivated and uploaded by wearable devices.[115]

But Congress enacted HIPAA long before wearable technology's potential healthcare benefits could be remotely imagined, and the law has been slow to adapt to new technologies.[116] While HIPAA might cover the personal health information cultivated and transmitted by wearable devices, because HIPAA's application is limited to "covered entities," its current regulations do not apply to most wearable technology manufacturers.

---

112. *See id.* at 4 ("I support the well-established Commission view that companies must maintain reasonable and appropriate security measures; that inquiry necessitates a cost-benefit analysis.").

113. *See* 45 C.F.R. § 160.103 (2014).

114. *See* 45 C.F.R. § 164.306 (2013); Health Insurance Reform: Security Standards, 68 Fed. Reg. 8334, 8334 (Feb. 20, 2003) (to be codified at 45 C.F.R. pts. 160, 162, 164).

115. *See* Ricardo Alonoso-Zaldivar, *Federal Health Privacy Law Leaves Consumer Data Vulnerable to Hackers*, REG.-GUARD (Feb. 6, 2015), http://registerguard.com/rg/news/32744498-76/federal-health-privacy-law-leaves-consumer-data-vulnerable-to-hackers.html.csp (HIPAA "remains the foundation for healthcare privacy in the Internet age.").

116. *See id.* ("Insurers aren't required to encrypt consumers' data under a 1990s federal law that remains the foundation for healthcare privacy in the Internet age—an omission that seems striking in light of the major cyberattack against Anthem.").

1. Strategic Marketing Limits HIPAA's Application to Wearable Devices

The HIPAA Privacy Rule protects individually identifiable personal health information that is transmitted by or maintained in electronic media on behalf of covered entities.[117] HIPAA defines "protected health information" as "any information . . . recorded in any form or medium, that . . . [i]s created *or received* by a healthcare provider . . . and . . . [r]elates to the past, present, or future physical or mental health or condition of an individual."[118] HIPAA defines "electronic media" as "storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium."[119]

Many wearable devices record individually identifiable personal health information in electronic form. The Apple Watch, for example, uses an accelerometer and built-in heart rate sensor to "provide a comprehensive picture of [a user's] daily activity."[120] The Watch also includes an activity application that "measures three separate aspects of [user] movement: calories burned, brisk activity and how often [a user] stands up during the day."[121] As such, it is reasonable to conclude that many current wearable devices record individually identifiable "protected health information" as defined by HIPAA.

Furthermore, technology manufacturers are partnering with software developers to help consumers use wearable devices to share their personal health information with doctors.[122] For example, in September 2015, Apple announced the creation of Airstrip, a HIPAA-compliant Apple Watch application that allows "patients and doctors to stay up to date about each other's statuses in real time."[123]

---

117. *See* 45 C.F.R. § 160.103 (2014).

118. *Id.* (emphasis added).

119. *Id.*

120. *Apple Unveils Apple Watch—Apple's Most Personal Device Ever*, APPLE (Sept. 9, 2014), http://www.apple.com/pr/library/2014/09/09Apple-Unveils-Apple-Watch-Apples-Most-Personal-Device-Ever.html [hereinafter *Apple Watch*].

121. *Id.*

122. David F. Carr, *Apple Partners with Epic, Mayo Clinic for HealthKit*, INFO. WEEK (June 3, 2014 1:40 PM) http://www.informationweek.com/healthcare/mobile-and-wireless/apple-partners-with-epic-mayo-clinic-for-healthkit/d/d-id/1269371.

123. Steve Smith, *Apple's Tim Cook Unveils Two New Medical Apps for Apple Watch That Bring Doctors, Patients Closer Together*, MED. DAILY (Sept. 9, 2015, 6:03 PM), http://www.medicaldaily.com/apples-tim-cook-unveils-two-new-medical-apps-apple-watch-bring-doctors-patients-351874.

"A rapidly aging global population in many industrialized countries accompanied by an increase in chronic diseases and the high cost of managing such diseases has led many to turn to a technological solution to ease the burden on healthcare professionals."[124] Wearable devices endeavor to solve this problem by creating a conduit between patients and doctors; channeling comprehensive personal health information directly from a user's body to a doctor's database.

But the most popular wearable devices purport to collect personal health data exclusively on *consumers'* behalf, rather than on behalf of physicians or other covered entities. The Apple Watch, for example, records "calories burned, brisk activity and how often [a user] stands up during the day," allowing a user to "see [his or her] activity history in greater detail."[125] Because manufacturers fail to officially acknowledge that wearable device consumers could (and, in fact, have already begun to)[126] share personal health information with physicians, most devices fall outside HIPAA's purview.

2. Wearable Device Manufacturers Are Not "Business Associates" Under HIPAA

The HIPAA Privacy Rule regulates the disclosure of identifiable personal health information made by business associates of covered entities.[127] In January 2013, HIPAA expanded its "business associate" definition to include any person who "[o]n behalf of [a] covered entity . . . creates, receives, maintains, or transmits protected health information for a function or activity . . . including . . . data analysis, processing or administration."[128] Now, "business associates" include parties that "provide[] data transmission services with respect to protected health information to a covered entity and require[] access on a routine basis to such protected health information."[129] Thus, HIPAA treats entities that maintain protected

124. Harry Rhodes, *Accessing and Using Data from Wearable Fitness Devices*, AHIMA http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050743.hcsp?dDocName=bok1_050743 (last visited Mar. 15, 2016).

125. *Apple Watch*, *supra* note 120.

126. *See* Amy Standen, *Sure You Can Track Your Health Data, But Can Your Doctor Use It?*, NPR (Jan. 21, 2015, 7:10 AM), http://www.npr.org/sections/health-shots/2015/01/19/377486437/sure-you-can-track-your-health-data-but-can-your-doctor-use-it ("[Dr. Paul] Abramson is a primary care doctor in San Francisco and lots of his patients work in the tech industry. So it's not surprising that more and more of them are coming in with information collected from consumer medical devices.").

127. *See* 45 C.F.R. § 160.102 (2013); 45 C.F.R. § 160.103 (2014).

128. 45 C.F.R. § 160.103 (2014).

129. *Id.*

health information on behalf of healthcare providers as "business associates"—and no longer "mere conduits"—regardless of whether the protected health information is actually accessed.[130]

Despite HIPAA's expanded definition, however, most wearable device manufacturers are not yet considered business associates of covered entities. Again, manufacturers utilize strategic marketing language to posit that wearable devices collect personal health data exclusively for consumers' use, rather than on behalf of physicians or other covered entities.[131] Notwithstanding the data's potential medical benefits, manufacturers avoid HIPAA's "business associate" regulations by deliberately failing to recommend that wearable device consumers share their personal health information with physicians.

Furthermore, when HIPAA has threatened to apply to wearable devices, manufacturers have shifted the responsibility for HIPAA compliance to other parties, including researchers and software developers. For example, Apple's ResearchKit invites software developers to innovate clinical research applications to interface with the Apple Watch.[132] Apple requires developers to "ensure that each participant is fully informed about the nature of the study, and . . . obtain a signed consent from each participant."[133] When an application falls under existing HIPAA regulations, Apple requires the *researcher* to maintain HIPAA compliance.[134] Thus, if Apple Watch violates HIPAA regulations by failing to securely collect or store personal health information for ResearchKit applications, Apple has seemingly absolved itself of responsibility, while other parties shoulder the liability.

130. *See* Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules, 78 Fed. Reg. 5566, 5572 (Jan. 25, 2013) (to be codified at 45 C.F.R. pts. 160, 164) ("[A]n entity that maintains protected health information on behalf of a covered entity is a business associate and not a conduit, even if the entity does not actually view the protected health information.").

131. *See Apple Watch*, *supra* note 120.

132. *See* RESEARCHKIT, http://researchkit.org (last visited Mar. 14, 2016).

133. *Obtaining Consent*, RESEARCHKIT, http://researchkit.org/docs/docs/InformedConsent/InformedConsent.html (last updated Jan. 11, 2016).

134. *See ResearchKit Framework Programming Guide*, RESEARCHKIT, https://developer.apple.com/researchkit/researchkit-technical-overview.pdf (last updated Jan. 11, 2016) ("Keep in mind that ResearchKit currently doesn't include . . . [a]utomatic compliance with international research regulations and HIPAA guidelines. These are the researcher's responsibility.").

V. RECOMMENDATIONS

Wearable technology is evolving rapidly; innovation dramatically outpaces existing federal regulations. As manufacturers develop wearable devices to record additional personal health information, enhanced personal monitoring promises tantalizing health benefits, but simultaneously implicates deepening consumer privacy concerns. Under the current regulatory scheme, lawmakers struggle first to understand the ever-shifting consumer electronics landscape, and then to apply antiquated regulations to new technologies. Stated bluntly, wearable technology threatens consumer privacy to such an extent that it requires regulation, but the legislative process moves too slowly to meet this need. Therefore, Congress is not in the best position to establish a comprehensive framework—or overhaul existing federal regulations—to protect consumer privacy and data security.

A. Congress Should Create a Federal Agency to Regulate Internet Privacy and Data Security

Congress should establish a standalone, cabinet-level department to coordinate and unify national Internet privacy and data security efforts. A single department can align the current patchwork regulatory structure to effectively protect both consumer privacy and data security on national networks.

Congress has, in the past, created federal agencies in response to similar concerns. For example, President George W. Bush proposed the Department of Homeland Security to meet "[t]he changing nature of the threats facing America" in the wake of the September 11 attacks on the World Trade Center.[135] In that instance, President Bush argued that America required a "single, unified homeland security structure [to] improve protection against [current] threats and be flexible enough to help meet the unknown threats of the future."[136] For the Bush administration, September 11 served as an essential tipping point in that it demonstrated a need for unification of homeland security within a single government agency.

Wearable technology represents a similar tipping point for privacy and data security. Wearable devices cultivate and store

135. GEORGE W. BUSH, THE DEPARTMENT OF HOMELAND SECURITY 1 (2002), http://www.dhs.gov/sites/default/files/publications/book_0.pdf.

136. *Id.*

expanding volumes of personal health information, exposing consumers' private health records to cybercriminals without any regulatory protection. Manufacturers are actively enhancing these devices to record additional personal health data points, obfuscating the line between "low risk" and federally-regulated devices.[137] All the while, personal health information is increasing in value by showcasing the personal statistics that allow data possessors to manage, market, or manipulate consumers more effectively.

Wearable technology will continue to evolve, for better and worse, and Congress should respond proactively by creating a single federal agency to regulate privacy and data security in real time. By coordinating experts in general technology, network security, engineering, and other relevant fields under a unified leadership, Congress could ensure progressive solutions to developing technological threats.[138] Furthermore, such an agency could guide the growth of wearable technology with greater agility and flexibility than the legislative process allows.

B. Congress Should Update HIPAA to Cover Wearable Devices

In the alternative, Congress should update HIPAA to cover current and future developments in wearable technology. Because HIPAA establishes federal standards to regulate the types of uses and disclosures of personally identifiable health information, it is currently in the best position to protect the data cultivated by wearable devices. But Congress enacted HIPAA long before wearable technology's benefits to human health could be remotely imagined, and as such, it has become outdated. Therefore, a large gap exists between the legal requirements that govern the health data collected for a consumer's personal use and the data collected as part of a relationship with a HIPAA-covered entity.[139]

To realize its full potential, wearable technology must cross the

137. *See FDA Draft Guidance*, *supra* note 93, at 2 ("[The Center for Devices and Radiological Health] does not intend to examine low risk general wellness products.").

138. *See* Establishment of the Federal Privacy Council, Exec. Order No. 13,719, 81 Fed. Reg. 7687, 7687 (Feb. 12, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-02-12/pdf/2016-03141.pdf (President Obama's recent Federal Privacy Council, created to establish an "interagency support structure" that allows the Government to "uphold the highest standards for collecting, maintaining, and using personal data," is an encouraging step toward the development of such a federal agency.).

139. Morgan Brown, *What Developers Need to Know About HIPAA Compliance in Wearable Tech*, TRUEVAULT: BLOG (May 14, 2014), https://www.truevault.com/blog/what-developers-need-to-know-about-hipaa-compliance-in-wearable-tech.html.

divide from "consumer electronics device" to "regulated medical device."[140] To accomplish this, HIPAA must evolve to establish regulatory standards for protecting consumer privacy and securing the personal health information collected by wearable devices.

Furthermore, if HIPAA can be enhanced to regulate standards for anonymizing personal health information, the big data generated by wearable devices can have significant epidemiological value. If personal health information can be shared anonymously with centralized processing databases, doctors can utilize this data to measure sociological health statistics in mass-scale clinical studies. The capacity to analyze comprehensive data sets and merge multiple data sources will be fundamental to solving important public health problems on the horizon. Evolved HIPAA regulations could establish guidelines for sharing this information between technology companies and statistical data centers. Apple Watch users, and users of other wearable devices, will generate health data that can benefit society at large. An enhanced regulatory scheme could establish guidelines for manufacturers' processing and sharing this consumer information.

HIPAA's privacy rule should expand to acknowledge that wearable devices collect "protected health information" on behalf of "covered entities." Many wearable devices record individually identifiable personal health information in electronic form. These devices should be regulated under HIPAA because consumers could (and, in fact, have already begun to)[141] share this personal health information with physicians.

Furthermore, wearable device manufacturers should be considered "business associates" of covered entities. By expanding HIPAA's definition to include entities that create, receive, maintain, or transmit protected health information on behalf of covered entities,[142] Congress impliedly acknowledged that future medical records will exist and be shared electronically. Wearable technology, and continued innovation in the collection of personal health information by wearable devices, will help create real-time electronic

140. *See* Nilesh Chandra & Chris Steel, *Wearable Tech Regulated as Medical Devices Can Revolutionize Healthcare*, MED. DEVICE & DIAGNOSTIC INDUS. (June 18, 2014), http://www.mddionline.com/article/wearable-tech-regulated-medical-devices-can-revolutionize-healthcare-6-18-2014.

141. *See* Standen, *supra* note 126.

142. 45 C.F.R. § 160.103 (2014).

health records, which will, in turn, improve patient care. In addition, wearable device manufacturers should share the burden for HIPAA compliance with researchers and software developers because wearable devices store and transmit personal health information. As such, further extension to designate wearable device manufacturers as "business associates" under HIPAA is appropriate.

VI. CONCLUSION

As wearable technology's benefits become more apparent, so too grow potential threats to consumer privacy and data security. The current federal regulatory scheme fails to address the evolving risks that inhere to wearable devices collecting and transmitting personal health information. The problem is multi-faceted; current statutory regulations are outmoded, and technological innovation moves far too quickly for the legislative process to keep pace.

Furthermore, because wearable technology aspires to improve human health, perhaps society has a vested interest in exploring the industry's potential to expand notions of traditional medicine. Creating a new federal agency to provide oversight, or updating existing HIPAA guidelines, will foster an environment through which consumers can adopt wearable devices with greater confidence as to the privacy and security of their personal health information. Moreover, with a regulatory framework providing clear parameters, wearable technology will be free to grow to obtain new kinds of health information, to interpret it in new ways, and to share it within the healthcare community with greater ease.