Wearable Fitness Devices: Personal Health Data Privacy in Washington State

Steven Spann[*]

CONTENTS

INTRODUCTION

Private entities are increasingly targeting individuals in the United States and around the world to gather personal data for such purposes as product development, market identification, and insurance risk assessment. While credit card records and online browsing histories have long

[*] J.D., Seattle University School of Law, 2016. Special thanks to all those who made this Note possible.

been the medium through which this data is gathered,[1] in more recent years, wearable fitness devices have added a new dimension to data production and collection. These devices are capable of gathering a significant amount of data regarding a person's physical and physiological characteristics,[2] thereby exposing these data producers to personal privacy infringement. Washington State lawmakers and citizens must be proactive in orienting themselves to the challenge of protecting personal health data derived from wearable fitness devices, and they must develop a framework of legal safeguards to protect individuals.

Wearable fitness devices, as the name implies, are generally on or attached to a person's body as a bracelet, watch, or token.[3] These products utilize sensors to track, and otherwise monitor a broad range of activities[4] performed by the user and generally transfer collected data to smartphones, computers, or network storage clouds.[5] Most, if not all, of this personal health data is transferred to entities outside the control of the data producer, including the device's manufacturer or a third party.[6] While such sharing of data is becoming increasingly common—and, some might argue, expected—in our electronics-driven culture, individuals are neither adequately informed regarding the scope of the data col-

1. *See* PAULA SELIS ET AL., WASH. STATE ATT'Y GEN.'S OFFICE, CONSUMER PRIVACY AND DATA PROTECTION: PROTECTING PERSONAL INFORMATION THROUGH COMMERCIAL BEST PRACTICES 3 (2002), *available at* http://digitalarchives.wa.gov/WA.Media/do/60F6041FBD01BC45F57915BCF83C59CD.pdf (noting that businesses can create databases of consumer-specific information such as "social security and credit card numbers, bank and credit card balances, and buying habits—as well as records of [the consumer's] online browsing activity," to enable better marketing strategies).

2. Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 101–02 (2014) (explaining that wearable fitness devices can accurately track daily steps, distances walked or run, calories burned, sleep duration and quality, heart rate, perspiration, skin temperature, and swimming speed and distance, as well as specific activities including basketball, skiing, surfing, weight-lifting, and rock-climbing).

3. *See Smartwatches and Smart Bands Dominate Fast-Growing Wearables Market*, CCS INSIGHT (Aug. 2014), http://www.ccsinsight.com/press/company-news/1944-smartwatches-and-smart-bands-dominate-fast-growing-wearables-market [hereinafter *Smartwatches and Smart Bands Dominate*].

4. *See* Peppet, *supra* note 2, at 102.

5. *See Frequently Asked Questions: What Data Is Stored on My Tracker, in the App, or on My Phone? Can I Control What Is Shared? What If I Want to Delete My Data?*, JAWBONE, https://jawbone.com/fitness-tracker/up3 (last visited May 22, 2016) (explaining that when the Jawbone wearable fitness device is synced, "all of your data is stored in the [Jawbone] app or in the Cloud"); Zuriñe Dopacio González, *The New Smart Wristbands for 2015*, WEARABLE TECHNOLOGIES (Feb. 10, 2015), https://www.wearable-technologies.com/2015/02/the-news-smart-wristbands-for-2015 (describing several Fitbit fitness devices that sync automatically with a smartphone or computer).

6. *See* Peppet, *supra* note 2, at 162 ("Typically, each sensor, and its associated data, is under the control of its manufacturer.") (citations and quotes omitted).

lection, transfer, and use, nor are they adequately protected by the law from exploitative behavior by these data users.

Federal and state governments play an important role in regulating the type of data that may be collected, the method of collection, and how and when the data may be transferred to third parties. The federal government retains broad authority to regulate the creation, storage, and transfer of certain data, including protected health information. However, given the scope and rate of data collection and transfer,[7] technology frequently exceeds the protections afforded by current federal law.[8] Furthermore, while federal law may provide a foundation for protecting such personal data, these laws may not afford the protections necessary for each state's citizens due to state-specific consumer technology use, privacy interests, and long-term consumer protection goals.[9]

As a result of these state-specific concerns, state governments should take concrete steps to deal with the privacy interests of their citizens. State governments are in the best position to promote individual protection against personal health data infringement by promoting tighter controls on protected data classifications. In this regard, Washington State lawmakers and citizens should put in place constitutional amendments and state legislation that promote personal privacy protection against data infringement. In the absence of such action, Washington's commitment to personal privacy may be rapidly undermined by the collection and use of personal health data.

---

7. *See id.* at 99 (discussing growth in the health and fitness device market); *see also infra* Part I.A.

8. *See* Press Release, Senator Charles E. Schumer, Schumer Reveals: Without Their Knowledge, Fitbit Bracelets & Smartphone Apps Are Tracking Users Movements and Health Data That Could be Sold to Third Parties; Calls for FTC to Require Mandatory Opt-Out Opportunity Before Any Personal Data Can Be Sold (Aug. 10, 2014), *available at* http://www.schumer.senate.gov/newsroom/press-releases/schumer-reveals-without-their-knowledge-fitbit-bracelets-and-smartphone-apps-are-tracking-users-movements-and-health-data-that-could-be-sold-to-third-parties-calls-for-ftc-to-require-mandatory-opt-out-opportunity-before-any-personal-data-can-be-sold [hereinafter Schumer Press Release]; *see also* Ariana Eunjung Cha, *The Human Upgrade: The Revolution Will Be Digitized*, WASH. POST (May 9, 2015), http://www.washingtonpost.com/sf/national/2015/05/09/the-revolution-will-be-digitized (describing the phenomenon of health tracking and noting the inadequacy of current federal regulation in protecting personal data derived from health tracking devices).

9. States are in the best position to identify how to address the needs of their respective citizens. For example, Washington State recently enacted a law to increase the consumer-notification requirements for data breaches. *See* E.S.H.B. 1078, 64th Leg., Reg. Sess. (Wash. 2015) (enacted). This law was heralded as providing "one of the strictest [data breach] notification requirements, practically requiring organizations across the country to notify all citizens (whether or not in Washington) in accordance with its directives." Jeffrey Cox & Aravind Swaminathan, *Washington State Poised to Set the Bar for Data Encryption Standards and Breach Notification*, JD SUPRA BUS. ADVISOR (Mar. 19, 2015), http://www.jdsupra.com/legalnews/washington-state-poised-to-set-the-bar-f-67343.

This Note addresses the nature and consequences of health data infringement by private entities, and the position that Washington State lawmakers should take in protecting against this infringement. Part I of this Note discusses the benefits and problems associated with wearable fitness devices and personal health data. Part II reviews the current federal approach to personal health data protection. Part III presents recommendations for Washington State constitutional amendments and legislative enactments that would protect Washington citizens against infringement of this data privacy. Finally, this Note concludes with a summary of the need for, and possible approaches to, protecting personal health data.

I. A STARTING POINT: WEARABLE FITNESS DEVICES AND HEALTH DATA

A. Fitness Devices and a Basis for Popularity

The popularity of wearable fitness devices has exploded since their entry into the consumer market.[10] According to one study, more than 30% of consumers plan to purchase a wearable fitness device in the next five years.[11] In fact, analysts predict orders for these "smart wearables" to reach 135 million units in 2018—up from 9.7 million in 2013[12]—with "wrist-worn devices [accounting] for 87% of wearables to be shipped in 2018."[13] Based on current trends, consumers are expected to purchase 68 million smartwatches[14] and 50 million smart bands[15] in 2018.[16] To develop a valid, workable solution to the problem of infringement of personal

10. *See* Press Release, NPD Group, Wearable Tech Device Awareness Surpasses 50 Percent Among US Consumers, According to NPD (Jan. 17, 2014), *available at* https://www.npd.com/wps/portal/npd/us/news/press-releases/wearable-tech-device-awareness-surpasses-50-percent-among-us-consumers-according-to-npd [hereinafter NPD Group].

11. Aditi Pai, *Survey: Fitness Devices to Be Most Popular Wearable for Next Five Years*, MOBI HEALTH NEWS (Nov. 13, 2014), http://mobihealthnews.com/38214/survey-fitness-devices-to-be-most-popular-wearable-for-next-five-years.

12. *Smartwatches and Smart Bands Dominate*, *supra* note 3.

13. *Id.*

14. "Smartwatches" are watches—frequently web-enabled—that indicate time and allow for fitness tracking, voice and text communication, and downloading apps, among other functionalities. *See* Alex Colon, *The Best Smartwatches of 2016*, PCMAG (May 9, 2016), http://www.pcmag.com/article2/0,2817,2456595,00.asp (providing overview of smartwatches from such manufacturers as Apple, Motorola, Pebble, and Samsung).

15. "Smart bands" include Fitbit and Jawbone bracelets. *See generally* FITBIT, https://www.fitbit.com (last visited May 22, 2016); JAWBONE, https://jawbone.com (last visited May 22, 2016).

16. *Smartwatches and Smart Bands Dominate*, *supra* note 3 (noting that smart bands generally have no screen or a limited display). Shipment projections vary between sources, but projections generally show major increases in wearable fitness device sales over the next several years. *See* Cha, *supra* note 8 (graphically portraying the past and projected sales of smart devices and apparel, and showing that smart band and sports watch sales are expected to reach 50 million and more than 40 million, respectively, by 2020).

data derived from wearable fitness devices, lawmakers and citizens must consider why consumers are interested in and use this technology as well as why private entities want this technology to be widely adopted.

Wearable fitness devices generally fall into a class of technology known by a variety of names, including mobile health (mHealth) technology.[17] MHealth technology can include a variety of wearable and non-wearable devices, whether they are used for "diagnosis, treatment, or simply well-being and maintenance."[18] Identifying the classification and capabilities of wearable fitness devices is an important basis for protecting personal data derived from these devices, and it provides insight into the appeal of these devices to individuals and private entities.

1. Medical and Social Benefits

To device users, the appeal of wearable fitness devices stems largely from these devices' medical and social benefits. MHealth technologies as a whole have the potential "to improve the quality of health care and reduce medical errors; to reduce the cost of health care; and to increase access to care by democratizing and demystifying medicine."[19] The quality of medicine can be improved and errors can be reduced through this technology because health care providers are able to provide more efficient, effective, and personalized treatment processes for patients who use these devices.[20] Through fitness devices and other mHealth products, medical professionals can utilize large-scale medical data[21] identified through such products to treat patients based on each patient's actual symptoms or physiological conditions.[22]

---

17. *See generally* 3 WORLD HEALTH ORG., GLOBAL OBSERVATORY FOR EHEALTH SERIES, MHEALTH: NEW HORIZONS FOR HEALTH THROUGH MOBILE TECHNOLOGIES 6 (2011), *available at* http://www.who.int/goe/publications/goe_mhealth_web.pdf. MHealth is defined as "medical and public health practice supported by mobile devices, such as mobile phones, patient monitoring devices . . . and other wireless devices." *Id.* Furthermore, in the context of Internet-linked electronic sensors, wearable fitness devices are also referred to as "Internet of Things" technology. *See generally* Peppet, *supra* note 2.

18. Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1176 (2014).

19. *Id.* at 1192.

20. *See id.* at 1192–93. Data production by these tracking technologies "will allow us to gather more granular health data on patients, and in shorter, more frequent intervals. Patients and providers can then use this data to better tailor care, to better coordinate care, and to avoid duplicative or unnecessary care." *Id.*

21. *See id.* at 1193 ("The intuitive appeal of mobile technologies is that they might leverage massive amounts of clinical research data and experience, embodying the ideals of empirical, 'evidence-based medicine.'").

22. *See* Timothy S. Hall, *The Quantified Self Movement: Legal Challenges and Benefits of Personal Biometric Data Tracking*, 7 AKRON INTELL. PROP. J. 27, 27–28 (2014) ("The potential benefits of health-related data tracking and data mining" include aggregation of user data to "predict health risks and disease outbreaks," and thereby "improve public health responses to such outbreaks, save lives, and improve efficiency of service delivery . . . . [The] collecting, sharing, and analyzing

In addition to the ability to address single-patient health problems, medical providers are able to use data from this technology to study the context in which specific health problems occur on a societal level.[23] With increased information precision comes increased insight regarding "societal habits and health issues, broken into handy categories like location, gender and age range."[24] This data can inform medical providers of correlative health trends—for example, the association between exercise and certain sleep habits, and links between location and the occurrence of weight-related illnesses—on a regional and national scale.[25] If updated at frequent intervals, such technology can also keep health care providers ahead of possible illness trends and concerns.[26]

Likewise, health care costs may be reduced through fitness devices because such technology has the potential to reduce the number of visits, or revisits,[27] to health care providers.[28] For example, where a patient is able to track sleep patterns at home—and thereby monitor when and how often they wake during the night and whether other biological characteristics accompany the sleep patterns—rather than in a hospital or outpatient setting, that initial data may provide meaningful insight into effective treatment without disrupting the patient's regular activities and without the use of expensive inpatient diagnostic processes.[29] Thus, if patients can send their personal health data directly to a health care provider without actually travelling to the provider's office, or such providers can prescribe treatment or recommend a particular wellness regime without having the patient wait in the provider's office, the costs of health care can be significantly reduced.[30] This type of treatment is especially valuable for patients in rural or underserved communities.

---

of individual health data can . . . provide those individuals with a level of insight about their health-related behaviors that is not easily achievable through other means.").

23. *See* Brian Heater, *Wearables Don't Just Let Us Compete With Strangers, They Let Us Peep on Them Too*, DIGITAL TRENDS (Sept. 1, 2014), http://www.digitaltrends.com/opinion/wearables-hold-possibilities-privacy-concerns/.

24. *Id.* ("It's easy to see how health organizations would be champing at the bit for that kind of data in an age of out-of-control obesity, diabetes, and other controllable health risks."); *see also* Hall, *supra* note 22, at 27.

25. *See* Hall, *supra* note 22, at 27–28 ("The potential benefits of health-related data tracking and data mining are vast and expanding. At the macro level, there can be benefits in using the aggregated data of millions of individuals to predict health risks and disease outbreaks.").

26. Cortez, *supra* note 18, at 1193 (stating that "[c]onstant monitoring might give [health care] providers more lead-time to respond to life-threatening conditions, or even predict them ahead of time, and could reduce hospital readmission rates").

27. *Id.* (discussing the benefits of monitoring by health care providers that could include a "reduc[tion in] hospital readmission rates").

28. *Id.* at 1195.

29. *Id.* (noting that "mobile technologies could reduce the number of hospital visits, physician visits, and other expensive fact-to-face consultations").

30. *Id.*

Further, in a democratization of medicine, "[m]obile health aspires to shift the locus of care away from [the] more established, expensive institutions [including physicians and other health care providers], and towards individual patients."[31] Where patients have more access to medical information—including sleep quality and duration, heart rate, body temperature, and caloric activity—and can analyze their own real-time health in light of that medical information, those patients can dramatically increase their understanding of personal health and thereby take action to address illness. The ability to share that real-time data can also aid other individuals in understanding their own health and the effectiveness of a particular treatment regime.[32]

Many individual consumers of wearable fitness devices also use this technology for more simple or practical reasons, including general self-monitoring, tracking, and sharing the data derived from this tracking with friends and family through social network systems.[33] These devices produce data that is paperless and easily transferrable, and allow individuals to observe data as they produce it.[34] Thus, fitness devices provide significant benefits that patients and health care providers seek to utilize in the context of health diagnosis, treatment, and well-being.[35]

2. Commercial Benefits

Private entities that use this consumer-produced data are also highly interested in the potential of wearable fitness devices. Forecasted as a "key consumer technology," more than 45 million wearable fitness devices are expected to be shipped in 2017.[36] As discussed earlier, the larger category of smart wearables, which include smartwatches and smart bands, is expected to reach 135 million orders by 2018.[37] All of this shipment activity will result in major commercial benefits for device manufacturers and other entities. The wearable fitness device market has

---

31. *Id.* at 1197.

32. *See* Cha, *supra* note 8 (explaining that individuals who regularly track their own health data often share their data "for the greater good"—approximately 34% of "health trackers share their data or notes with someone else").

33. *See generally* Hall, *supra* note 22 (discussing the "Quantified-Self" movement); *see also* Cha, *supra* note 8 ("[Wearable health] technology is inherently social. Many users share their body metrics with friends, family, and even co-workers as readily as they would pictures from their travels to distant countries or their late-night bar adventures.").

34. *See The UP System*, JAWBONE, https://jawbone.com/up (last visited May 22, 2016).

35. *See Hall*, *supra* note 22, at 29 (stating that proponents of fitness devices and apps "predict that this unprecedented exercise of healthcare consumer autonomy will have dramatic effects on the way in which healthcare is practiced, virtually ending the practice of medicine as we know it"); *see also* Cortez, *supra* note 18, at 1176.

36. Press Release, Canalys, 1.6 Million Smart Bands Shipped in H2 2013 (Feb. 12, 2014), *available at* http://www.canalys.com/newsroom/16-million-smart-bands-shipped-h2-2013.

37. *Smartwatches and Smart Bands Dominate*, *supra* note 3.

grown to over $330 million,[38] with the industry created by these wearable technologies—including products from Fitbit[39] and Jawbone[40]—forecasted to produce sales of $50 billion by 2018.[41]

In addition, the predictive value of personal health data incentivizes the production of wearable fitness devices.[42] Current data collection and analysis processes[43] now allow the "exploration of information . . . to identify connections and relationships that are unexpected or were previously unknowable."[44] With wearable fitness device data, private entities and individuals are able to utilize the data produced by these devices to establish statistical inferences,[45] such as credit worthiness, insurance risk, and employment or academic qualification.[46] Additionally, a growing number of employers are using fitness devices to encourage corporate wellness[47] in order to "create [a] culture of well-being," "improve participant health status," "increase employee productivity," and "boost acquisition and retention."[48] Thus, according to some sources, the medical, social, and commercial benefits weigh heavily in favor of relatively un-

38. NPD Group, *supra* note 10 ("Among likely buyers, counting calories (50 percent) and tracking the numbers of steps taken in a day (32 percent) are the most sought after features. Just 6 percent say they would be interested in sharing their fitness data on a social network.").

39. *See generally* FITBIT, https://fitbit.com/ (last visited May 22, 2016).

40. *See generally* JAWBONE, https://jawbone.com/ (last visited May 22, 2016).

41. Cha, *supra* note 8; *see also* Press Release, ABI Research, Led by the Sports, Fitness, and Wellness Segment, Wearable Wireless Device Revenues to Exceed $6 Billion in 2018 (Sept. 30, 2013), *available at* https://www.abiresearch.com/press/led-by-the-sports-fitness-and-wellness-segment-wea [hereinafter ABI Research Press Release] (providing early projections that indicated the sports, fitness, and wellness tracking devices will maintain at least a 50% share of wireless device shipments through 2018).

42. Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 77–79 (2014).

43. While the data collection and analysis processes produce benefits for the private entities, they cause the very privacy infringement problems that Washington State needs to address. *See infra* Part II.B.

44. Terry, *supra* note 42, at 78 (stating that because of the current data analytical processes' "potential to yield unanticipated insights, the dramatically low cost of information storage and the rapidly advancing power of algorithms have shifted organisations' priorities to collecting and harnessing as much data as possible and then attempting to make sense of it").

45. *Id.* at 79.

46. *Id.*

47. Adam Satariano, *Wear This Device So the Boss Knows You're Losing Weight*, BLOOMBERG TECH (Aug. 21, 2014, 10:26 AM), http://www.bloomberg.com/news/2014-08-21/wear-this-device-so-the-boss-knows-you-re-losing-weight.html (noting that "companies, facing rising health expenses, are increasingly buying and subsidizing fitness-tracking devices to encourage employees and their dependents to be more fit").

48. *Reasons to Invest in Wellness Go Beyond Health*, FITBIT, http://www.fitbit.com/fitbit-wellness#i.94b7aavy3cr3t0 (last visited May 22, 2016) (explaining the Fitbit Wellness corporate program).

encumbered wearable fitness device development.[49] However, the problems associated with the accessibility of data produced by wearable fitness devices cannot be ignored.

B. Wearable Fitness Devices and Data Privacy Problems

A number of distinct processes associated with wearable fitness device data pose significant problems to data privacy. These processes include data collection, producer-data correlation, security and disclosure, and accumulation.[50] These problem areas have developed over time and now serve as discrete, although far from exclusive, considerations in privacy legislation.[51]

A relatively recent example is illustrative of privacy problems surrounding wearable fitness devices. On August 24, 2014, a magnitude 6.0 earthquake occurred near Napa, California.[52] This earthquake was the largest earthquake in approximately twenty-five years, and caused extensive damage in Napa County.[53] The following day, Jawbone,[54] a manufacturer and provider of wearable fitness devices, aggregated and graphically presented sleep-pattern data from wearers of its Jawbone UP bracelet in areas surrounding Napa to the public through the company's blog.[55] The graphical display that accompanied this data presented Jaw-

---

49. Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, 3 (2015) ("[G]enerally speaking and barring clear evidence of direct risk to health or property—not merely hypothetical or ephemeral fears—policymakers should not impose prophylactic restrictions on the use of new wearable technologies and [Internet of Things].")

50. Some scholars refer to data accumulation as "aggregation," referring to the pooling of a particular user's data to develop a macro-level user "profile." *See* Anne Marie Helm & Daniel Georgatos, *Privacy and mHealth: How Mobile Health "Apps" Fit into a Privacy Framework Not Limited to HIPAA*, 64 SYRACUSE L. REV. 131, 149 (2014) (describing the data-related activities as "surveillance (unauthorized collection of user information), identification (connecting user information to his or her identity), insecurity (risking access by others by not encrypting data), disclosure (sending sensitive information to third parties), and aggregation (providing data to advertisers for the aggregation of a consumer profile)").

51. Scholars have categorized problems surrounding wearable devices as problems of discrimination, privacy, security, and consent. *See generally* Peppet, *supra* note 2.

52. Press Release, U.S. Geological Survey, Update on the Magnitude 6 South Napa Earthquake of August 24, 2014, (Aug. 25, 2014), *available at* https://www.usgs.gov/news/update-magnitude-6-south-napa-earthquake-august-24-2014.

53. *Id.*

54. *See generally* JAWBONE, *supra* note 40.

55. *See* Eugene Mandel, *How the Napa Earthquake Affected Bay Area Sleepers*, JAWBONE BLOG (Aug. 25, 2014), https://jawbone.com/blog/napa-earthquake-effect-on-sleep. According to Jawbone, 93% of UP wearers living in Napa, Sonoma Vallejo, and Fairfield (within 15 miles of the earthquake's epicenter) woke up at the time the earthquake occurred. Of the UP wearers in San Francisco and Oakland (farther from epicenter), 55% woke up at that time. At a distance of 75 to 100 miles from the epicenter, in Modesto and Santa Cruz, almost no UP wearers woke up during the earthquake.

bone's analysis of individuals who woke up at the time of the earthquake.[56]

This aggregation of personal health data, with Jawbone's analysis of why the individuals woke up, presents a number of problems for data privacy. Initially, assuming that UP wearers in fact consented to the use of their respective data in a public presentation, Jawbone neither offered evidence regarding the accuracy of the information, nor provided any basis for its conclusion that people awoke at that time as a result of the impact of the earthquake. Also, whether UP wearers were sufficiently informed as to the use of their personal health data raises concerns about the validity of their consent. The validity of informed consent as to the collection and release of personal health data is particularly problematic where device privacy policies, on which consent is based, are difficult to find; lack definitional uniformity—for example, the definition of "personal information" may vary by manufacturer; and frequently fail to identify who owns the produced data.[57] Even this example, in which all data was apparently "anonymized and presented in the aggregate,"[58] poses problems for personal health data privacy.

A number of specific limitations exist as to health data privacy protection, including consumer consent to the privacy and sharing policies of device manufacturers,[59] a lack of government action[60] in addressing rapid technological advances, data security from hackers,[61] producer-data "re-identification,"[62] and consumers' sharing[63] of personal health data.[64]

---

56. *See id.*

57. Peppet, *supra* note 2, at 140–48.

58. *See* Mandel, *supra* note 55.

59. *See* Peppet, *supra* note 2, at 140–48. Scholars and practitioners in the health care industry, and numerous other fields, have long wrestled with the issue of consumer consent, and whether the consumer has been meaningfully informed before consenting to a particular activity. In the context of personal data, like other fields, a party who consents to the access and sharing of personal information generally cannot bring an actionable claim for that infringement of privacy. *See* William Dalsen, *Civil Remedies for Invasion of Privacy: A Perspective on Software Vendors and Intrusion Upon Seclusion*, 2009 WIS. L. REV. 1059, 1071 (2009). Dalsen notes that "there is no intrusion where consent was granted to access another's information, or where others acquired information in an expected or usual way." *Id.*

60. *See* Schumer Press Release, *supra* note 8; *see also* Peppet, *supra* note 2, at 140 (stating that "consumer protection law related to privacy-policy disclosures is currently unprepared to deal with [the complicated nature of Internet of Things devices]").

61. Lisa Eadicicco, *A New Wave of Gadgets Can Collect Your Personal Information Like Never Before*, BUS. INSIDER (Oct. 9, 2014, 11:26 AM), http://www.businessinsider.com/privacy-fitness-trackers-smartwatches-2014-10.

62. Peppet, *supra* note 2, at 129 (citing Ira Hunt, Chief Tech. Officer, Cent. Intelligence Agency, The CIA's Grand Challenges with Big Data, Address at Gigaom Structure Data 2013 (Mar. 20, 2013), *available at* http://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data/2) ("[S]imply by looking at the data [from a Fitbit] they can find out . . . with pretty good accuracy what your gender is, whether you're tall or you're short, whether

Regardless of how an entity obtains an individual's personal health data, whether directly from the device wearer or from another source, that data could be used to legally or illegally restrict an individual's ability to access certain markets.[65] Through the use of personal data, entities could discriminate against an individual in employment,[66] health care and insurance,[67] and credit-based lending,[68] among other life necessities or options.[69] Likewise, predictive modeling can use a consumer's location, weight, activity level, gender, and even sleep data, in specific areas or in the aggregate, to develop consumer-specific, region-specific profiles for marketing purposes. As a result of these successful, "highly targeted and segmented advertising profiles and the delivery of . . . customized product offerings based upon consumers' individual interests,"[70] entities that collect and transfer this data to third parties have an extraordinary incentive to create more avenues through which consumers produce and share

---

you're heavy or light, . . . [and] you can be 100% . . . identified by simply your gait—how you walk.")) (alterations in Peppet).

63. Cultural expectations regarding the sharing of information, and the ubiquity of software privacy policies, which consumers frequently do not read, often promote a cycle of improper data sharing, collection, and misuse, leaving the consumer inadequately informed and protected.

64. Consumers making their own personal data available via social networks or other media is a significant limitation to the availability of protections for personal data. Where people knowingly share their own personal fitness or health-related data, their ability to have a meaningful remedy for any other person's use, or misuse, of data is significantly reduced. *See* Dalsen, *supra* note 59, at 1071 (explaining that "regardless of the format or medium, publicly available information cannot hide behind 'privacy' protections").

65. *See* Peppet, *supra* note 2, at 118 ("Currently, both traditional discrimination law and information privacy law, such as the [Fair Credit Reporting Act], are unprepared for such new forms of discriminatory decision making.").

66. *See id.* at 119 ("Fitbit data could reveal a great deal to an employer. Impulsivity and the inability to delay gratification—both of which might be inferred from one's exercise habits—correlate with [unhealthy lifestyles and financial conditions] . . . . Such information could tip the scales for or against [a] hypothetical candidate.").

67. *But see* Jena McGregor, *Fitness Trackers Chase After the Corporate Market*, WASH. POST (Dec. 18, 2014), http://www.washingtonpost.com/blogs/on-leadership/wp/2014/12/18/fitness-trackers-chase-after-the-corporate-market/ (stating that certain corporate wellness programs that use devices from Fitbit or Jawbone do not necessarily provide employee-specific data to the employers). For example, "Fitbit also only shares sleep data in the aggregate," and "Jawbone's Up for Groups [corporate wellness] program only shares information in the aggregate with employers." *Id.*

68. *See* Terry, *supra* note 42, at 79.

69. *See* Peppet, *supra* note 2, at 117–18 ("[M]assive amounts of sensor data from [personal-data producing] devices can give rise to unexpected inferences about individual consumers. Employers, insurers, lenders, and others may then make economically important decisions based on those inferences, without consumers or regulators having much understanding of that process. This could lead to new forms of illegal discrimination against those in protected classes such as race, age, or gender. More likely, it may create troublesome but hidden forms of economic discrimination based on [this] data.").

70. Dominique Shelton, *Online Behavioral Advertising: Tracking Users: Gold Mine or Land Mine?*, LANDSLIDE, Sept.–Oct. 2012, at 26, 27 (2012).

data, and thereby increase the quantity of those entities' marketable product—personal health data.

Ultimately, wearable fitness device users, medical professionals, data collectors, and end-users obtain benefits from this technology. It is clear, however, that the data producer—the individual—suffers significantly from an end-user's exploitation of the data. Individuals do not generally seek to have their personal health data used in public surveys, employment or insurance assessments, or creditworthiness analyses. Thus, the issue is much larger than one company merely identifying that some people were awake during an earthquake.

II. CURRENT FEDERAL LAW: A LIMITED LANDSCAPE

Depending on the nature and method of the data collection, and to whom that data is transferred, fitness and other mobile health devices are covered by a range of federal laws from various governmental entities, including the Department of Health and Human Services, the Federal Trade Commission, and the Food and Drug Administration.[71] However, one of the problems with this protective framework is that it largely covers only health, or otherwise personal, information that is transferred to or stored by a health care provider or the provider's business associates.[72] Likewise, some mobile health technology only falls within the purview of certain federal guidance if used to "diagnose, cure, treat, mitigate, or prevent specific, identifiable diseases or conditions."[73] As most fitness devices track sleep patterns, user location, and other activities not related to treating illness, and this information is not transferred to or stored by a health care provider, such devices are not covered by many federal health privacy laws.[74]

---

71. Cortez, *supra* note 18, at 1179.

72. *See* Helm & Georgatos, *supra* note 50, at 154 (noting that "[t]he HIPAA Privacy Rule only applies to health plans, health care clearinghouses, and health care providers who transmit any health information in electronic form in connection with a covered transaction—in other words, 'covered entities' or their 'business associates'").

73. *See* Cortez, *supra* note 18, at 1189–90. The article discusses FDA regulations and notes that the FDA is not primarily concerned with regulation of technologies that "allow[] users to log, record, and make decisions about their general health and wellness. This group [of apps] includes diet trackers, calorie counters, exercise regimens, and the like." *Id.*

74. *See* Cha, *supra* note 8 ("Federal patient privacy rules under [HIPAA] don't apply to most of [tracked data]. Unless the data is being used by a physician to treat a patient, the companies that help track a person's information aren't bound by the same confidentiality, notification and security requirements as a doctor's office or hospital.").

A. HIPAA and HITECH

The Health Insurance Portability and Accountability Act (HIPAA)[75] is considered one of the most fundamental federal health privacy protection statutes in place today.[76] This legislation was initially enacted in 1996 and "tasked the Department of Health and Human Services . . . [with] adopting standards of 'measures to be taken to secure [protected health] information while in the custody of entities covered by HIPAA . . . as well as in transit between covered entities and from covered entities to others."[77] Ultimately, HIPAA was designed to "improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery."[78] HIPAA has developed into a statutory framework that governs the transfer and storage of protected health information[79] and enforces health information protection through civil penalties.[80]

When HIPAA was enacted, it included a requirement that the Department of Health and Human Services develop "national standards for electronic health care transactions and code sets, unique health identifiers, and security."[81] The Department of Health and Human Services established a Privacy Rule in 2000, which required the protection of "individually identifiable health information" by specifically covered entities, including health plans, health care clearinghouses,[82] and health care pro-

---

75. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat 1936 (1996) [hereinafter HIPAA].

76. *See* Helm & Georgatos, *supra* note 50, at 152.

77. *Id.* at 152–53 (second alteration in original).

78. HIPAA, *supra* note 75.

79. "Protected health information" (PHI), according to the HIPAA framework, refers to "individually identifiable health information transmitted or maintained by a covered entity or its business associates in any form or medium." *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, U. S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#_edn2 (last visited on May 22, 2016) (paraphrasing 45 C.F.R. § 160.103 and noting that PHI includes "the individual's past, present, or future physical or mental health or condition," and such "identifiers" as "name, address, birth date, [and] Social Security Number . . . when they can be associated with the health information listed above [including physical or mental health]").

80. David J. Dykeman, Nancy E. Taylor & Jessica A. von Reyn, *Mobile Health Technologies Face a Changing Regulatory and Patent Landscape*, SCITECH LAW, Spring 2014, at 10, 13.

81. *HIPAA for Professionals*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative (last visited May 22, 2016) [hereinafter *HIPAA for Professionals*].

82. Under the HIPAA Privacy Rule,

> [h]ealth care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and 'value-added' networks and switches, that does either of the following functions: (1) Processes or facilitates

viders, and mandated the security of "protected health information."[83] Furthermore, a Security Rule was established in 2003, which "set[] . . . standards for protecting the confidentiality, integrity, and availability of electronic protected health information."[84]

As a supplement to HIPAA,[85] Congress passed the Health Information Technology for Economic and Clinical Health Act, known as HITECH, in 2009.[86] The Act was designed to "promote the adoption and meaningful use of health information technology . . . [and] address[] privacy and security concerns associated with the electronic transmission of health information."[87] HITECH also utilizes "mandatory penalties for 'willful neglect' leading to the exposure of health data" and ensures consumers are notified in the event of a data breach at the covered entity.[88]

Yet, as personal health data derived from fitness devices does not always consist of protected health information as defined by the HIPAA framework,[89] and the data produced is generally stored by, or transferred to or from, non-health care entities, as opposed to covered health care-related entities, the technology often falls outside of the purview of HIPAA and HITECH.[90]

B. Federal Trade Commission Regulations

Likewise, the Federal Trade Commission (FTC) has played a role in protecting the privacy of health data. Through various regulations[91] the FTC has broad "authority to police marketing practices, including decep-

---

> the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction. (2) Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

45 C.F.R. § 160.103 (2014).

83. *HIPAA for Professionals*, *supra* note 81.

84. *Id.*

85. Andrea L. Gothing, Seth A. Northrop & Li Zhu, *Taking the Pulse of Digital Health: Key Legal Issues Surrounding Wearable Technology*, INSIDE COUNSEL (Feb. 12, 2015), http://www.insidecounsel.com/2015/02/12/taking-the-pulse-of-digital-health-key-legal-issue.

86. Pub. L. No. 111-5, tit. XIII, 123 Stat. 115, 226 (2009).

87. *HITECH Act Enforcement Interim Final Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/hitechenforcementifr.html (last visited May 22, 2016).

88. Gothing, Northrop & Zhu, *supra* note 85.

89. *Id.* (noting that "personal health data stored on a wearable device, such as calories burned, is not subject to HIPAA"; although, transmission of the data to a health care provider might implicate HIPAA requirements).

90. *See* Cha, *supra* note 8.

91. Among these regulations are the Federal Trade Commission Act, Gramm-Leach-Bliley Act, Fair Credit Reporting Act, and the Children's Online Privacy Protection Act of 1996. Helm & Georgatos, *supra* note 50, at 159.

tive acts related to the collection, sharing, and use of consumer information"[92] and "to enforce data security laws tailored to more specific conditions."[93] Although the FTC has not provided overarching regulatory guidelines for health data protection, it has taken steps to ensure consumer data is protected, and, in the future, it will likely play a major role in ensuring the privacy of data derived from fitness devices.[94]

C. Food and Drug Administration Regulations

The Food and Drug Administration (FDA) has also played a role in regulating devices[95] used to produce health data.[96] In large part, the FDA's regulation of these devices is focused on ensuring the necessary functionality and safety of the devices' diagnostic, prescriptive, and autonomous medical capabilities.[97] However, FDA oversight of mobile health technologies has recently been focused more on the mobile applications (apps) of the technology.[98] This oversight provides the FDA with a degree of regulatory discretion for "lower risk" products, thereby ena-

---

92. *Id.*

93. *Id.*

94. *See* Schumer Press Release, *supra* note 8 ("There are currently no federal protections to prevent [wearable fitness device] developers from then selling [collected] data to a third party without the wearer's consent. Schumer therefore urged the Federal Trade Commission (FTC) to push fitness device and app companies to provide a clear and obvious opportunity to 'opt-out' before any personal health data is provided to third parties . . . ."); *see also Spring Privacy Series: Consumer Generated and Controlled Health Data*, FED. TRADE COMM'N (May 7, 2014), http://www.ftc.gov/news-events/events-calendar/2014/05/spring-privacy-series-consumer-generated-controlled-health-data (providing information presented at an FTC seminar discussing consumer health data production and privacy issues associated with this trend).

95. According to the Food, Drug, and Cosmetics Act, a "device" is,

> an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is—
>
> (1) recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them,
>
> (2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or
>
> (3) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes.

21 U.S.C. § 321(h) (2012).

96. *See* Dykeman, Taylor & von Reyn, *supra* note 80, at 12.

97. *Id.* at 11.

98. *See* FOOD AND DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF (2015), *available at* http://www.fda.gov/downloads/MedicalDevices/.../UCM263366.pdf (providing guidance regarding "how the FDA intends to apply its regulatory authorities to select software applications intended for use on mobile platforms (mobile applications or 'mobile apps')").

bling a more relaxed enforcement of FDA requirements.[99] Nevertheless, if a certain technology, whether medical device, application, or other product, falls within FDA coverage, the FDA generally requires that technology to meet specific standards before the technology can be sold to the public.[100]

Thus, because fitness devices pose a "low risk" to consumer safety and do not collect information used to "treat" a patient, the devices have largely gone unregulated.[101] This trend shows no signs of change in the near future, and, for this reason, Washington State must move forward in developing much needed protections of personal health data.

III. MOVING FORWARD: WASHINGTON PROTECTIONS

This Part proposes the statutory framework, including state constitutional amendments and legislation that Washington State should develop to protect consumers from privacy infringement through wearable fitness devices. Given that the magnitude of data mining and privacy infringement will only continue to increase as individuals create more personal data through these devices,[102] Washington needs to be proactive in addressing the protection of personal data, especially in the largely unregulated area of fitness devices.[103]

Although personal data privacy problems encompass a number of distinct activities, including data collection, correlation, security and disclosure, and accumulation,[104] these functional areas can be placed into two major fields of regulatory classifications relative to the time of data collection: upstream and downstream protections.[105] Upstream protec-

---

99. *See id.* ("Some mobile apps may meet the definition of a medical device but because they pose a lower risk to the public, FDA intends to exercise enforcement discretion over these devices (meaning it will not enforce requirements under the [Food, Drug, and Cosmetic Act]).").

100. *See* Dykeman, Taylor & von Reyn, *supra* note 80, at 11.

101. *See* Cha, *supra* note 8 (noting that current FDA regulations "would essentially leave hundreds, if not thousands, of 'low-risk general wellness' products—a category that presumably applies to the current incarnation of Fitbits—free from extra scrutiny under federal food and drug safety laws," and, in regard to HIPAA, explaining that "[u]nless the data is being used by a physician to treat a patient, the companies that help track a person's information aren't bound by the same confidentiality, notification and security requirements as a doctor's office or hospital").

102. *See supra* Part I.A.2.

103. Furthermore, Washington legislators should consider that privacy "interests [including personal dignity, autonomy, and self-determination] are served by giving people some control over others' acquaintance with their personal affairs. By exercising control over others' knowledge of ourselves, we can avoid judgment, ridicule, or stereotyping (preserving dignity) while we comfortably pursue the activities we would like (maintaining autonomy)." Jane Yakowitz Bambauer, *The New Intrusion*, 88 NOTRE DAME L. REV. 205, 213 (2012).

104. *See generally* Helm & Georgatos, *supra* note 50. These areas have also been described as a "'harmful activities' taxonomy," which consists of information collection, information processing, information dissemination, and invasion. *See* Terry, *supra* note 42, at 103.

105. *See* Terry, *supra* note 42, at 103.

tions cover those areas that fit into a "privacy" framework, limiting the value of data and restricting its collection.[106] The upstream category of data protections would include the collection and possible correlation of personal data privacy.[107]

On the other hand, downstream protections limit the storage and use of personal data and ensure data breach notification to data producers.[108] This field of data protections would cover information processing, disclosure, and accumulation processes of personal data use. Downstream protections also incorporate what has been termed "use constraints," or "don't use rules," by some scholars.[109] Such constraints have been applied frequently in other areas of the law, including constitutional, consumer crediting reporting, and health insurance law.[110] Ultimately, while the more protective route—either upstream or downstream—is debated in the field of data privacy,[111] some combination of the two should be used to maximize health data protection.

As a result of these considerations in data protection and the areas in which data infringement occurs, Washington State's approach to personal data protection should be more defined. Examples of the protective

---

106. *See id.*

107. *See generally* Peppet, *supra* note 2 (identifying data problems as related to discrimination, privacy, security, and consent). Protections that address privacy, security, and, in some cases, consent, would fall into the upstream classification, while those that address discrimination and, generally, consent would fall into the downstream classification.

108. Terry, *supra* note 42, at 103 (noting that downstream protections "include[] security requirements specifying physical and technological barriers to protect collected data, restrictions on the retention, disclosure, or distribution of collected information . . . and notification of breach rules when the data has been compromised").

109. Peppet, *supra* note 2, at 150 (stating that use constraints "rest on a social judgment that even if transacting parties both wish to reveal and use a particular piece of information, its use should be forbidden because of some social harm . . . that is greater than the social benefits, such as the allocative and contractual efficiency created by allowing freedom of contract").

110. *Id.* ("Use con-straints [sic]—or 'don't use' rules—are common across the law. Fifth Amendment jurisprudence prohibits a jury from drawing negative inferences from a defendant's failure to testify; the [Fair Credit Reporting Act] bars consumer reporting agencies from including bankruptcies more than ten years old in consumer credit reports; and the [Genetic Information Nondiscrimination Act] bars the use of genetic information by health insurers."). Downstream protections depend largely on the "context of the original data grant" as a basis for data usage. *See* Terry, *supra* note 42, at 103. However, when the data producer provides information to the data use, with a grant of authority to use that data to a certain extent, the scope of that consent is relatively clear. *Id.*

111. *See* Terry, *supra* note 42, at 104 (FTC Chairwoman Edith Ramirez stated that "[u]se restrictions have serious limitations and cannot, by themselves, provide effective privacy protection. Information that is not collected in the first place can't be misused. And enforcement of use restrictions provides little solace to consumers whose personal information has been improperly revealed."). Upstream data protection model provides more collection-centric protections such that less data is obtained by data collectors. *Id. But see* Peppet, *supra* note 2, at 151 (recommending the use of downstream, cross-context use constraints, which would prevent the use of personal data derived from one context—for example, health improvement—for purposes in another context-such as employment candidacy).

avenues that should be utilized to protect against data infringement include private tort actions in intrusion,[112] breach of contract claims,[113] consumer protection actions,[114] constitutional amendments,[115] and legislative protections that could be similar to those in other states—for example, California[116] and Texas.[117]

A. Constitutional Amendment

Although some degree of protection already exists in Washington State's constitution, more protection should be granted through amendments to the constitution. The State constitution is one of "a handful of state constitutions" that explicitly protects privacy.[118] In this regard, Washington's constitution articulates, "No person shall be disturbed in his private affairs, or his home invaded, without authority of law."[119] While this constitutional prohibition against invasion of private affairs or homes "is qualitatively different from the Fourth Amendment and provides greater protections,"[120] it has been largely interpreted against such invasion only by government entities.[121] This constitutional provision should be amended to extend protections against private intrusions and applied to personal health data privacy infringement by such private entities. In this way, consumers will be better protected against misuse of personal data that they do not want shared with others.

Washington lawmakers and citizens should consider California's constitution in developing protection of such data. California's constitution states, "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty,

---

112. *See generally* RESTATEMENT (SECOND) OF TORTS §§ 652B-E (1977); Bambauer, *supra* note 103; Dalsen, *supra* note 59; SELIS ET AL., *supra* note 1, at 14 (stating that "[c]ivil remedies for infringements on an individual's right to privacy are limited to the tort doctrines of false light, appropriation, private facts, and intrusion").

113. However, breach of contract claims regarding privacy policy violations face challenges in showing that actual damages resulted from the breach. Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 595–96 (2014) (discussing cases addressing privacy policy violations through breach of contract claims).

114. *See* Helm & Georgatos, *supra* note 50, at 158 (noting that, "[a]s a general matter, both state and federal consumer protection laws are more inclusive than other privacy laws, including both those related to communications and to health information because they are not similarly limited to specific entities or specific types of information").

115. *See infra* Part III.A.

116. Terry, *supra* note 42, at 91.

117. *Id.* at 91–92.

118. *Id.* at 90.

119. WASH. CONST. art. 1, § 7.

120. State v. Hinton, 319 P.3d 9, 12 (Wash. 2014).

121. *Id.* ("Article I, section 7 'is grounded in a broad right to privacy' and protects citizens from governmental intrusion into their private affairs without the authority of law.") (quoting State v. Chacon Arreola, 290 P.3d 983 (Wash. 2012)).

acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."[122] This article of the California constitution has been applied to private parties where the party at issue has infringed on the privacy interests of the plaintiff. In *Hill v. National Collegiate Athletic Association*,[123] the California Supreme Court held that California's "Privacy Initiative in article 1, section 1 of the California Constitution creates a right of action against private as well as government entities" for the infringement of personal privacy. [124]

B. Legislative Amendment

Legislative protection of data derived from wearable fitness devices should be based on the nature of the data—personal health data—rather than for what purpose the data is used, such as fitness improvement. Appropriate data protection, then, includes amending Washington's current health information protection laws, including RCW 70.02, and proceeding with additional legislated protections. Through these endeavors, both upstream and downstream facets of data protection would be addressed.[125]

Washington's Health Information Act is the State's primary health data protection legislation and was enacted in 1991.[126] Although this statute provides protection similar to HIPAA for traditional health care information, it does not necessarily address the non-traditional health care information and processes associated with wearable fitness devices.[127] Yet, because of the health-related nature of data derived from fitness devices, RCW 70.02 should provide the same, or similar, protections to this non-traditional health information.

Even though the statute would need to be modified to address personal health data as it relates to wearable fitness devices, the statute already includes features that pertain to these devices. For example, the statute provides that "[h]ealth care information is personal and sensitive information that if improperly used or released may do significant harm to a patient's interests in privacy, health care, or other interests."[128] This statute further states that "[p]atients need access to their own health care information as a matter of fairness to enable them to make informed de-

122. CAL. CONST. art. 1, § 1.

123. *See* Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994).

124. *Id.* at 644. *See generally* Pettus v. Cole, 57 Cal. Rptr. 2d 46 (Cal. Ct. App. 1996).

125. Also, while this Note does not specifically discuss data breach protection, this aspect of privacy would need to be addressed as well.

126. WASH. REV. CODE § 70.02 (1991).

127. For example, RCW § 70.02 does not address personal health data such as sleep patterns and activity levels. *See infra* notes 130–36 and accompanying text.

128. WASH. REV. CODE § 70.02.005(1) (1991).

cisions about their health care and correct inaccurate or incomplete information about themselves."[129] Guided by these findings, the Washington Legislature developed a set of protections, responsibilities, limitations, and enforcement mechanisms surrounding personal health information[130] that should now be developed further to address personal health data derived from wearable fitness devices.

Initially, the definitions[131] contained in the statute must reflect the change in health data protection.[132] Among the changes needed are a redefining of the terms "health care,"[133] "health care information,"[134] "health care provider,"[135] and "patient."[136] An amended definition of "health care" should specifically reflect that such care, or services, includes those services conducted for the purpose of monitoring a physical or mental characteristic, including sleep and location of the subject person by a wearable or implantable device.[137] Likewise, the definition of "health care provider" would need to account for entities engaged in some level of collection, analysis, and interpretation of personal health data derived from these devices.

Other states, including California and Texas, have similarly established legislation that provides some means of addressing health information protection.[138] California's Confidentiality of Medical Information Act[139] attaches HIPAA-like data protection to "health data custodians

129. WASH. REV. CODE § 70.02.005(2) (1991).

130. *See generally* WASH. REV. CODE § 70.02 (1991).

131. *See* WASH. REV. CODE § 70.02.010 (1991) (amended 2014).

132. *See* Peppet, *supra* note 2, at 138–39 (discussing the defining of "personal information" for greater protections of wearable fitness device data).

133. "'Health care' means any care, service, or procedure provided by a health care provider: (a) To diagnose, treat, or maintain a patient's physical or mental condition; or (b) That affects the structure or any function of the human body." WASH. REV. CODE § 70.02.010(14) (1991) (amended 2014).

An amended definition could reflect that the care or service includes those for the purpose of monitoring the condition of the patient by a redefined "health care provider" entity.

134. "'Health care information' means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and directly relates to the patient's health care, including a patient's deoxyribonucleic acid and identified sequence of chemical base pairs. The term includes any required accounting of disclosures of health care information." WASH. REV. CODE § 70.02.010(16) (1991) (amended 2014).

135. "'Health care provider' means a person who is licensed, certified, registered, or otherwise authorized by the law of this state to provide health care in the ordinary course of business or practice of a profession." WASH. REV. CODE § 70.02.010(18) (1991) (amended 2014).

136. "'Patient' means an individual who receives or has received health care. The term includes a deceased individual who has received health care." WASH. REV. CODE § 70.02.010(31) (1991) (amended 2014).

137. This would provide a more "whole-health" understanding of protected health information, rather than the limited understanding presently in use.

138. Terry, *supra* note 42, at 90–91.

139. CAL. CIV. CODE §56 (1981).

who are not health care providers."[140] In this way, the sharing and use of health data by non-health care provider entities is covered by the legislation. Likewise, Texas's health data protection legislation[141] specifically addresses "'any person who engages in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting protected health information.'"[142] Thus, definitional amendments to RCW 70.02 to reclassify health information to include health data derived from fitness devices would provide the necessary groundwork to guide subsequent health data protection development.

Additional components of amended health information protections in Washington should include a requirement that device users be allowed to specify what and how data is to be shared with third parties at the initial setup of their device, with the option to change these specifications at any time.[143] In addition, amendments should provide that data producers have access to their respective data at any time;[144] that the sale and sharing of data be specifically restricted; and that manual, consumer-initiated sharing of specific data may occur.[145] Such legislation would afford the necessary protections through civil penalties and private actions[146] and yet still allow data-user entities to obtain consumer data when the data producer permits.

As discussed above, Washington's health data privacy laws must account for upstream and downstream needs. Through this proposed legislation, the upstream protection would be derived from the reclassification of protected personal data and by ensuring that the device user is able to opt out of data sharing. The downstream protection would be af-

---

140. Terry, *supra* note 42, at 91.

141. Medical Records Privacy Act, TEX. HEALTH & SAFETY CODE § 181 (2011) (amended 2012).

142. Terry, *supra* note 42, at 91–92 (quoting Medical Records Privacy Act, TEX. HEALTH & SAFETY CODE ANN. § 181.001(b)(2) (West 2010 & Supp. 2012)). "Texas also requires 'clear and unambiguous permission' before using health information for marketing and broadly prohibits the sale of an individual's protected health information." *Id.* at 92.

143. Schumer Press Release, *supra* note 8.

144. Peppet, *supra* note 2, at 161–62 ("[I]n a recent study of Fitbit, Withings scales, and other health-related sensor devices, [researchers] found that users want to be able to have a copy of the data such devices produce. This is the simplest level of control over one's data—the ability to inspect, manipulate, and store your own information."). *But see* WASH. REV. CODE § 70.02.080 (1991) (amended 1993) (requiring health care providers to provide for a "patient to examine or copy all or part of the patient's recorded health care information").

145. This standard may be similar in some aspects to the "property approach" to privacy in which data producers may refrain, or "hold out," from sharing their data "if it is important to them, even if that choice seems irrational. A property system favors the autonomy and self-determination of information subjects over competing interests, such as information access and economic efficiency." Bambauer, *supra* note 103, at 217.

146. *See* WASH. REV. CODE § 70.02.170 (1991) (allowing civil remedies for violation of statute).

forded by regulation of this data sharing through specific limitations on data sharing and sale. Considering that Washington already protects data in a variety of forms, including protection of credit report data[147] from improper sharing,[148] as well as motor vehicle recording device information,[149] personal data derived from fitness devices should be afforded similar protections.

C. Ramifications

As discussed above, mobile fitness devices and the data that they produce are high-value business interests, and they will only increase in value.[150] Likewise, at least a portion of the data derived from these devices is beneficial to medical knowledge as a whole and is beneficial specifically to the individuals who use the devices.[151] Yet, the advantages of these wearable fitness devices must be balanced with the value of personal privacy and the knowledge that, once lost, this privacy is difficult to regain. While increased regulation could result in reduced access to protected data and, therefore, reduced business profits for data collectors, long-term privacy protection is a socially and personally valuable commodity that must be protected.

CONCLUSION

Wearable fitness devices promote the production, storage, and transmission of personal health data. As a result of various data analytics processes used by device developers, data consumers, and other third parties, personal data from these devices has become a valuable commodity for use in predictive marketing, health care and insurance, and other largely unrestricted intrusions on personal privacy. Washington State should be proactive in protecting its citizens' privacy interests and take innovative steps to prevent organizations and individuals from improperly collecting and sharing personal data. In this regard, Washington legislators should enact specific laws that afford increased regulatory control over data collection and use processes as well as increased avenues for individuals and groups of consumers to pursue private rights of action against infringing entities.

---

147. *See* Peppet, *supra* note 2, at 151–52 ("[S]everal states, including California, Connecticut, Hawaii, Illinois, Maryland, Oregon, and Washington, have passed laws limiting employers' consideration of credit reports, even though research has shown that credit scores correlate with traits such as impulsivity, self-control or impatience, and trustworthiness.").

148. *See* WASH. REV. CODE § 19.182.020 (1993) (amended 2007).

149. *See* WASH. REV. CODE § 46.35 (2009); Peppet, *supra* note 2, at 154–55.

150. *See supra* Part I.A.2.

151. *See supra* Part I.A.1.