The Privacy, Security and Discoverability of Data on Wearable Health Devices: Fitness or Folly?

Vishakha Kumari and Sara Anne Hook(✉)

Department of Human-Centered Computing, Indiana University School of Informatics and Computing, 535 W. Michigan Street, Indianapolis, IN 46202, USA
vkumari@umail.iu.edu, sahook@iupui.edu

Abstract. With data from wearable health devices increasing at a rapid rate, it is important for lawmakers to make sure that this data remains well protected. This paper will question the perceptions of people with respect to current and future use of wearable health devices, especially if the security and privacy risks to their data are more commonly understood, and particularly if this data is discoverable and admissible in court. It will explore the electronic discovery issues with data from wearable health devices in the context of litigation and examine how the current rules of court procedure and evidence would be applied. The paper will review the federal and state legislation that may or may not provide protection for data from wearable health devices. The authors intend to use their paper as a vehicle to advocate for stronger statutory protection and greater clarity about the use of and potential risks to this data, including when the data becomes evidence in litigation.

Keywords: Wearable health devices · Fitness devices · Internet of Things (IoT) · Privacy · Security · Electronic discovery · Legislation

1 Introduction

Wearable health and fitness devices are emerging at a rapid rate and the lives of people are being impacted by them. On one hand, these wearable health devices help a user to achieve his/her health goals and improve overall health by constantly tracking and monitoring health data. However, the lack of clear legislative protection for the privacy and security of this data can put individuals at risk. What the future of this industry will be like is not known. However, it will be interesting to evaluate if this technology will have a positive or negative impact on people's lives. To narrow the scope of this paper, it will specifically focus on fitness trackers rather than trying to cover the full range of health devices that are available.

The paper will first review the federal and state legislation that may or may not provide protection for data from wearable health devices and advocate for either new legislation or amendments to existing statutes that would offer at least some level of security and privacy over this data. It will explore the electronic discovery issues with data from wearable health devices in the context of litigation and examine how the current rules of court procedure and evidence would be applied. It will highlight the

M. Antona and C. Stephanidis (Eds.): UAHCI 2017, Part III, LNCS 10279, pp. 50–64, 2017.
DOI: 10.1007/978-3-319-58700-4_5

perceptions of people with respect to current and future use of wearable health devices, especially if the security and privacy risks to their data are more commonly understood, and particularly if this data is discoverable and admissible in court. The authors hope to raise the awareness of the HCI and health informatics communities so that these professionals will be more mindful of the issues when designing and testing wearable health devices and in using these devices themselves. They intend to use their paper as a starting point to advocate for stronger statutory protection and greater clarity about the use of and potential risks to this data, including when the data becomes evidence in litigation.

2 Wearable Health Devices and Their Data

It has been estimated that one in every ten Americans over the age of eighteen owns an activity tracker [1]. The wearables market has shown impressive growth over the years and is expected to increase to 35% by 2019 [2]. This growth rate speaks to the growing interest in wearable technology. The wearables industry is promising a healthier future with devices capable of monitoring daily activities, calories burned, sleep patterns, body temperature, step counts, heart rate, oxygen levels, hydration levels and blood sugar levels, to name but a few [3]. These wearable health devices perceive and record information about users continuously and discreetly. With every second, the amount of health-related data available through the Internet is increasing. Wearable health devices are considered as being part of the Internet of Things (IoT), which "involves not only the connection and integration of devices that monitor the physical worlds – temperature, pressure, altitude, motion, proximity to something else, biometrics, sound, images, and so forth – but also the aggregation, relationship and analysis of the information those devices create in order to take action on the situation, and the business and technology

Fig. 1. Example of a Fitbit

changes required to use the data and analyses" [4]. As indicated in Fig. 1 of this report, the Internet of Things "stack" can be represented as a triangle, with local sensing at the bottom, then data integration and analytics of things, with cognitive action at the top of the pyramid [4]. As the authors note in their discussion of what this means for an IoT application, "[w]ithin the activity tracker industry, for example, the end-state vision should address how consumers, the health and fitness industry, and the health insurance industry will make use of the devices, functions, and data" [4].

2.1 Advantages of Health Data from Wearables

The advent of these wearable health devices offers the potential to dramatically alter the way that health care services are delivered because of the opportunity for users and providers to more easily capture, compare and respond to even small changes in a person's medical status, hopefully before the person's condition worsens. These devices can reduce the visits to clinics and hospitals and can perhaps reduce overall expenses on health care. These devices allow remote health monitoring, which is particularly worthwhile for chronic conditions and elder care. Wearable health devices not only benefit the consumer, but they can also help health care service providers to facilitate and improve the quality of care. If the data can be aggregated, it has the potential to bring a health revolution and transform the health industry. Aggregated data from wearable devices can provide valuable insights into the overall health of the population and the collective data can be used to plan for the facilities, personnel and expenditures that

Fig. 2. Screenshot of user's cellphone with Fitbit data

will be needed in the future. Moreover, many of these wearable health devices, particularly fitness trackers, are attractive and easy to use and provide a very simple view of the user's data on his/her cellphone (Fig. 2).

2.2 Concerns with Wearable Health Devices

In 2015, personal health information breaches affected 113 million individuals and with the wearable market on the rise the breach rate is bound to increase if measures are not taken [5]. The reason for this is that health information is 50 times more profitable on the black market than Social Security numbers [6]. Also, the use of wearable devices brings the possibility of this data being exposed to the black market since these devices tend to be easy to compromise in a socio-technical sense. The data collected by these devices are either stored locally, or if collected ubiquitously, then stored in a cloud. There can be physical theft, malware attack or loss of local data and these devices are not yet sophisticated enough to provide a secured flow of the data to the cloud, which can act as another hacking point [7].

2.3 Security and Privacy Concerns

Wearable devices generate and store confidential health information about the user, because of which there is a high chance of misuse if the privacy and security of this data are not ensured. The scenario that the decision to promote someone was based on the data collected by a fitness tracker that was given to an employee by his/her employer is now a possibility. As has been seen with other high-profile information security breaches, inadequate protection of this data can put people who use wearable devices at greater risk for becoming victims of identity theft, profiling, stalking, extortion or discrimination at a personal and professional level [8]. Bad credit, inaccurate health records, higher premiums and loss of insurance coverage are a few other examples of problems which may arise [7].

2.4 Electronic Discovery

Although questions about evidence in digital format were raised in cases as early as the 1980s and 1990s, the emerging area of law known as electronic discovery (e-discovery) did not begin to find its way into the typical lawyer's lexicon until the mid-2000s. Two major events occurred during this time that marked the true beginning of the field of e-discovery and that continue to form the foundation of how the process is handled today. In *Zubulake v. UBS Warburg*, Judge Shira A. Scheindlin articulated major principles and themes regarding e-discovery, including the responsibilities of lawyers and clients, sanctions for spoliation of evidence and what constitutes accessible versus inaccessible data [9]. In 2006, the Federal Rules of Civil Procedure were amended to incorporate Judge Scheindlin's rulings and to establish the discoverability of Electronically Stored Information (ESI) as an umbrella term intended to encompass both current and future technology and the data that it generates. E-discovery is something that impacts everyone, whether they know if or not, because it deals with the proper collection,

preservation, analysis and production of evidence in digital form. To put it bluntly, in the United States, if you are sued, the opposing party's lawyer will request nearly every piece of digital evidence in any format that might be relevant to the case, including email, text messages and information from social media sites. Anyone can find himself/herself needing to comply with requests for potentially relevant evidence – in electronic or paper/hard copy form. There are various steps in an e-discovery process which are best understood by reviewing the Electronic Discovery Reference Model (EDRM).

As indicated by the EDRM below, the duty to preserve potentially relevant ESI begins at the time that litigation can reasonably be anticipated rather than when actual notice is received about a lawsuit, investigation or audit. Ideally, an organization - or even an individual - will be managing its information appropriately even beforehand so that the actual e-discovery process will be as streamlined as possible. For users of wearable health devices that generate data that may be relevant to a case, the challenges will be knowing that they need to preserve this data, how to identify the data that may be requested and then how to properly collect this data. Of course, the lawyer representing the user should be able to offer guidance. The scenario of needing to obtain information from a user's wearable health device can be compared with that of information from social media sites. Although it would be tempting to think that data from wearable health devices can be requested and received from the vendors of these devices or cloud computing services that might be storing this data, in the context of social media, commentators suggest that it is best to first make the requests for information from the actual users or from other users ("friends") who may have access to this data. Thus, it will be interesting to see what procedures are developed for requesting data from wearable health devices, particularly the valuable information that might show trends in a user's medical status, activity levels or location (Fig. 3).

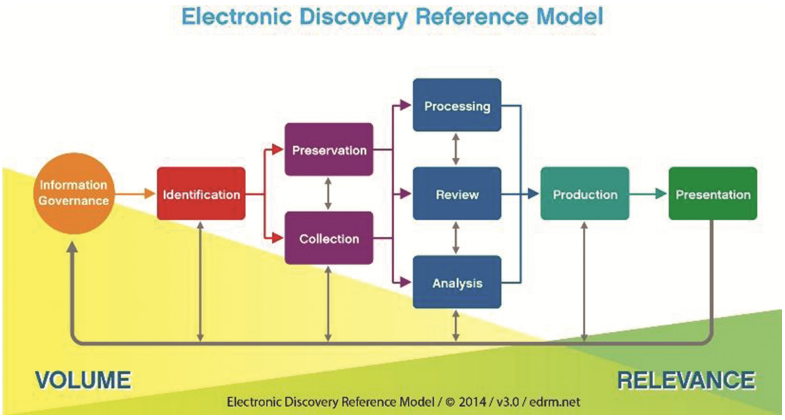

Fig. 3. Electronic Discovery Reference Model (edrm.net)

The Federal Rules of Civil Procedure were amended again in December 2015 to shorten the timeframes for various stages in an e-discovery process, to place a greater emphasis on proportionality and to provide clarity on when and what kinds of sanctions

the court can impose for spoliation of evidence [10]. Courts are already applying the amended version of the Federal Rules of Civil Procedure, which means that an e-discovery process must now be completed in a significantly reduced period of time and with greater specificity required for requests and objections [11]. The e-discovery process becomes increasingly complex as lawyers and clients deal with wearable devices and the Internet of Things, which create and store even more potentially relevant electronic evidence in a wider variety of files and formats [12, 13].

Thus, another concern with data from wearable health devices is that it will usher in a new era of digital forensics because these devices present a rich repository of potentially relevant evidence that can be requested and used as part of litigation. As with other Electronically Stored Information (ESI), courts are already allowing data from these devices to be discovered and admitted in trials [14, 15]. Even though data from wearable health devices is discoverable, it must still meet the tests for admissibility as outlined in the Federal Rules of Evidence and corresponding state court rules. One of the issues with the data generated by wearable health devices is its reliability, especially since studies indicate that the readings may not be entirely accurate [16, 17]. The variety of wearables available in the market have their own algorithms to track and capture data. For some, even moving one's leg while seated is captured as a step taken, while other devices give a different result because the wearable was probably too tight or loose on the wrist to record the data properly. Determination of deep from light sleep has different parameters for each of the fitness tracking devices. For data which lacks standardization to be used as evidence can be perilous to the objectivity of the judicial system. Similar to concerns with social media, one of the special issues with data from wearable health devices is authenticity, since it would have to be proven that the person to whom the device is attributed was actually the one using it [18].

As previously indicated, the data from a fitness device was used in the case of a 44-year-old woman who claimed she had been awakened and sexually assaulted at around midnight. The data from her fitness device showed she was awake and walking at the alleged time of the crime. She first claimed to have been wearing her fitness device during the time of the attack, but later changed her story to having lost her wearable device during the attack [19]. Later, it was shown that she falsified the entire incident and was ordered to serve two years of probation and complete 100 h of community service. Another case was of a Canadian law firm which collected the fitness data of its client to compare that to other wearers of her age and profession to show that the plaintiff's activities were reduced from what would normally be expected due to the injuries she sustained in an auto accident [20, 21].

Concerns have also been raised about instances where employers and insurance companies have provided wearable devices such as fitness trackers under the auspices of promoting the health and wellness of employees and insureds [22, 23]. Although seemingly benevolent at first glance, is such data collection over-intrusive and would it result in either adverse employment actions or denial of coverage for illnesses or injury if someone could point to a lack of physical activity as a rationale? Although wearable health devices, which collect data continuously, might be able to give a picture of what might have happened, they may fail to collect the exact details of the particular moment. However, the data from wearable health devices including fitness trackers does present

a rich repository of potentially relevant evidence, particularly for cases involving personal injury, medical malpractice, employment disputes and any other type of litigation where someone's health status is at issue. Trend data will be especially valuable. Lawyers have been searching for and requesting information from social media sites for several years, looking for data about opposing parties, the lawyers who represent them, potential jury members and judges and even their own clients so it is unlikely to be any different with data from wearable health devices. One of the authors has been publishing articles and book chapters and giving presentations on e-discovery for 10 years. Most recently, she reviewed a number of recent cases that considered a wide variety of files and formats of information in digital form, including social media, email, video surveillance, chats and instant messages [24]. It is clear that data from wearable health devices will be considered Electronically Stored Information (ESI) for purposes of discovery. However, data from wearable health devices will still need to meet all of the other requirements outlined under the Federal Rules of Evidence and comparable state court rules in order to be admissible in court.

3 What U.S. Federal Legislation May Apply to Fitness Devices?

There is an urgent need for the legal framework to catch up with the speed of technology development; the gap between the law and technology continues to widen. Unfortunately, research suggests that neither the Health Information Portability and Accountability Act (HIPAA) - nor any other federal or perhaps even state law - seems expansive enough to protect the health data collected by these devices. The wearables industry is such a rapidly-evolving field that there are no specific sets of laws that cover it. The public seems unaware of the security and privacy risks posed by wearable health devices; however, this may change if there are some high-profile instances of misuse of this data. Fortunately, experts are calling for new regulations, including legislation that would cover the health and fitness data of employees [25].

3.1 HIPAA and the HITECH Act

Health information that is captured and stored by wearable health devices such as fitness trackers is likely not considered protected health information under federal or state law unless the information is shared with doctors, hospitals or any third-party vendors (Business Associates) of these entities. Because these devices are not covered under the Health Care Portability and Accountability Act (HIPAA), there can be little to no expectation of privacy or security provided under this legislation. Interestingly, one major vendor of wearable devices indicates that its devices are HIPAA-compliant, raising questions about why this vendor chose to incorporate HIPAA considerations into its products when other vendors have not done so [26]. Without adequate statutory protection, questions remain about whether the use of wearable health devices actually promotes fitness or is folly.

In addition, the advancement in technology today makes it very easy to re-identify data and link it back to the person. However, under HIPAA, the data falls out of the

protection scheme once it is de-identified, since protection is only available for "individually identifiable data" [25].

In 2009 another law, known as the HITECH Act, considered a more refined version of HIPAA, was passed to "addresses the privacy and security concerns associated with the electronic transmission of health information" [27]. However, even the reforms to this law do not encompass data from wearable health devices and thus this data falls out of the protection provided by these laws.

Concerns about the security and privacy of individually identifiable health information are not confined to the wearable devices industry, but are more broadly considered whenever technology is used to create, store and transmit health data. Indeed, Rockwell notes that "[t]he telemedicine industry is especially vulnerable to exposing private patient information given its reliance on electronic data collection and storage and frequent distant data transfer" [28]. The author examines the application of HIPAA and the HITECH Act of 2009 in the context of telemedicine, noting that the question of "whether a patient-facing telemedicine technology vendor is a HIPAA business associate subject to these regulations is a complex question depending on a number of variables" [28]. Additionally, she observes that "[e]lectronic health records, video storage devices, telemedicine devices, and any other data-generating or receiving device involved in the telemedicine interaction carries the potential to collect and store protected health information" [28]. As she concludes, "[c]ollection and storage of that information as well as any use or disclosure are subject to federal HIPAA and HITECH laws [28]. It is fairly easy to apply the same approach to the collection and storage of data from wearable health devices.

3.2 Federal Trade Commission (FTC)

The Federal Trade Commission (FTC) ensures that consumers should be able to enjoy the benefits that technology brings without having to worry about the privacy risks involved. Though not specifically directed towards health data, the FTC sets guidelines for protecting consumer data. In the future, it can play an important role in protecting the data from wearable health devices. The federal rules will have to be adjusted to encompass wearable devices and to ensure that consumers are not misled about the privacy protections in place for their data. As is clear from a number of FTC enforcement actions, vendors and other third parties that are part of the wearable health devices industry will have to be careful not to "overpromise" about the security and privacy practices that are used to safeguard the data that is generated, stored, transferred and shared about consumers. Particularly worrisome to many consumers is the specter of "secondary use" of their data by third parties without permission or without an opportunity to "opt out" of certain activities such as data collection and analysis and offers for additional services from third party vendors.

3.3 Food and Drug Administration (FDA)

The Food and Drug Administration (FDA) is another U.S. agency charged with protecting and promoting public health through the control and supervision of regulated

medical devices. Fitness trackers likely would be placed into the category of "low risk general wellness" devices and thus do not require FDA oversight [29]. However, when the use of fitness trackers is recommended by physicians, they would fall under FDA's purview as now they can be classified as medical devices and thus could be regulated by it.

The FDA has made it clear that it does not intend to regulate "low risk" devices, but as wearable technology delves deeper into the realm of tracking and monitoring as part of bona fide medical services to maintain a patient's health, there is a need to regulate these devices as well [30].

4 Representative Examples of State Legislation that May Apply to Fitness Trackers

The authors chose three states to examine to see whether there is legislation available that could potentially provide more protection for the security and privacy of data from wearable health devices such as fitness trackers than what is available at the U.S. federal level.

4.1 Indiana

The authors are currently located in Indiana, so they were first interested in reviewing the potential legislation that might be available in this state that would offer a greater level of protection for the security and privacy of data from wearable health devices than what is provided under federal law. Indiana Code 24-4.9 covers the disclosure of a security breach, which includes definitions for terms such as breach of the security of data, data base owner, encrypted data, "person" and personal information, requirements for disclosure and notification of a breach, the duties of a database owner, the methods of disclosure, penalties for disclosure and the actions that can be taken by the Attorney General [31]. Indiana Code 4-1-6 features its Fair Information Practices and Privacy of Personal Information [32]. Finally, Indiana Code 4-6-14 is devoted to the protection of health records and identifying information [33].

4.2 Massachusetts

The law in Massachusetts was the second state of interest to the authors. Many experts consider the laws in Massachusetts that deal with information security and privacy to be the best among all of the states in the United States. Moreover, these experts advocate for other states to adopt what Massachusetts has in place, hopeful that it can be a model not only at the state level but also the federal level. The law in Massachusetts includes regulations on the protection of personal information. Its definitions for "persons" and "personal information" are expansive [34]. Its Standards for the Protection of Personal Information of Residents of the Commonwealth cover purpose and scope, definitions, duty to protect and standards for protecting personal information and a deadline of March 1, 2010 for compliance [35]. Interestingly, this statute includes computer system security

requirements, making it particularly compelling as guidance for implementing a comprehensive security program [35]. Among the provisions within this section of the statute are secure authentication protocols and secure access control measures that include education and training of employees [35].

4.3 Washington State

Fortunately, as this paper was being developed, a comprehensive examination of the personal health data privacy laws that would apply to wearable fitness devices was published in the *Seattle University Law Review* [30]. The author first provides an explanation for why fitness devices are so popular, including the medical and social benefits of these devices and the commercial benefits [30]. The author then discusses the current federal law, including HIPAA and the HITECH Act and the regulations from the Federal Trade Commission (FTC) and the Food and Drug Administration (FDA), characterizing them as a "limited landscape" [30]. He proposes a statutory framework, including state constitutional amendments and legislation, that Washington State should develop to protect consumers from privacy violations through wearable fitness devices [30].

The Uniform Health Care Information Act, enacted in 1991, is Washington's state primary health data protection legislature. It recognizes the patient's interests in privacy and health care and states 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" [36]. It also focuses on the rights to access health care information, stating that "[p]atients need access to their own health care information as a matter of fairness to enable them to make informed decisions about their health care and correct inaccurate or incomplete information about themselves" [36]. Washington State's current health information protection laws provide protection similar to HIPAA for traditional health care information and the state constitution is considered one of "a handful of state constitutions that explicitly protects privacy" [30]. However, the law needs to expand and be more definitive in order to provide better protection for personal health information and the processes associated with fitness devices.

5 Recommended Next Steps

The rate of growth of the wearable industry demands a quick update in the design and legal framework of these devices to avoid the misuse of this data. In this part of the paper, the authors will cover design considerations and legal reforms which would help to ensure the health data remains secure and can act as permissible digital evidence if needed. They consider what other approaches that can be taken to provide greater comfort to users of wearable health devices and to the vendors and third parties who provide these devices or handle the data generated by them.

5.1 Design Amendments

Security should be a prime concern for the professionals designing wearable health devices. The responsibility to make sure that data is safe should rest upon the hands of consumers as well as the designers, makers and vendors of these devices. The industry can show respect for a user's data by making the private settings as the default settings of these devices and giving users the freedom to choose otherwise. The user's expectation that his/her data is safe and not being shared with third parties without his/her consent should be met. Secondly, how often has it happened that the user did not understand a vendor's Terms of Service or Privacy Policy, and yet agreed its terms and conditions just for the sake of obtaining the devices or using the software application. It is unlikely that in such cases the user will pack up his/her wearable health device and return it. The designer's intervention is needed in fashioning an application where the user has the choice to opt out of any terms and conditions, yet he/she will still retain the basic functionality of the device. Wearables provided to users as medical devices is a potential solution, but again there should be an update on the legislative side.

In addition, keeping users informed about the specific data being generated and stored and how this data is going to be shared with any third party would be an important step forward. This can be accomplished during the initial setup; however, the design should always allow users to go back, check and change their information sharing settings and other preferences whenever they choose.

5.2 Law Amendments

The law must keep pace with the growth and innovation in the wearable health devices industry. It is still unclear what laws and regulations apply to this ever-evolving field. There is a need for specific laws targeted towards the "wearables" which will ensure that the privacy, security and discoverability of this data is clearly defined. It is important that protocols for requesting, collecting and preserving health data from wearable health devices be clarified, likely through court cases as well as amendments to federal and state court rules, so that clients and their lawyers handle this data properly throughout the e-discovery process, but particularly during the identification, preservation and collection stages.

Previously, the authors discussed the definitions of "covered entities," "individually identifiable health information" and "third parties." To extend HIPAA protection to data from wearable health devices, it is necessary to expand the above-mentioned definitions of this terminology, such as including device manufacturers as covered entities, and encompassing in the definition of business associates all of the involved third parties that store, share and analyze the data from these devices. In addition, broadening the scope of "individually identifiable health information" to include the data from the wearable devices and mobile health applications will prepare data from wearables for being admissible and discoverable in the digital age.

5.3 Other Options

Interestingly, insurance companies are now providing coverage for devices and data falling under the broad umbrella heading of the Internet of Things (IoT). As indicated by Reuhs, the "internet of things" appears to "represent the next wave of new liabilities: cars being remotely controlled by hackers; medical devices being used as access points for theft of medical records; baby monitors being used as spying devices; a software update pushing bad code that disables a fire sprinkler system; and TVs being rendered useless by malware" [37]. The article continues with a description of general liability policies and what they might cover and exclude related to IoT devices and the data they capture and store. As he indicates, since 2014, nearly all commercial general liability polices have excluded coverage for non-physical loss arising from data breaches (whether from IoT devices or not) [37]. He then discusses whether first-party losses would present more interesting insurance issues, noting that because all of these issues may not be solved in a larger sense, it is important to read policies carefully and understand the risks [37].

There is an overall lack of awareness about what kinds of data are being generated by wearable health devices and who can access it. The relative newness of this technology has not yet offered users with an opportunity to explore and become more vigilant about the protection of their data, especially given the variety of privacy threats that can emerge because of the continuous collection, storage and sharing of this data. The ubiquitous nature of these devices makes it difficult for users to be able to perceive the potential risks. The lack of privacy awareness in ubiquitous systems was a problem identified in early research; however, controlling privacy had been the prime focus rather than increasing privacy awareness of users [38, 39]. The design of these wearable health devices should be such that the visibility of information transfer is more transparent. One way to do this is by making an intuitive and easy to access user interface featuring relevant privacy information. Adding data control filters would be another way to ensure that users have some decision-making power over what data is collected, when it is collected, how much will be collected and shared and who will have access to it. This will make users more conscious of the data that is being shared and give them more control over the data that they prefer to share, making the data sharing process a more intentional act. A society that is well-informed and updated on the privacy and security issues that might arise because of wearable health devices will provide an incentive for designers, manufacturers and vendors to incorporate security measures as an integral part of their wearable health device systems.

Another important facet of addressing the risks with wearable health devices such as fitness trackers is user education. Although Fitbit provides extension information on its privacy policies, it is unlikely that users either read or understand what these policies mean [40, 41]. One of the authors was twice offered a free fitness tracker as part of the wellness programs on her campus, which she refused because of concerns about privacy, security and e-discovery. Participants were not provided with any information about these issues nor with suggestions for how to secure their data. Moreover, the leaders of the wellness program were shocked when the author told them that the data from fitness trackers was already being requested as evidence as part of litigation. Some options for

increasing a user's awareness of the risks that might be posed by wearable health devices include clearer and more succinct privacy policies posted on vendor websites and training that accompanies the distribution of these devices as part of medical, health and wellness initiatives. The information on the Fitbit website is noteworthy in that the first set of information is in summary form in non-legal language that the public can easily understand [40]. More detailed information is then included as part of the company's detailed Privacy Policy [41]. Fitbit also provides its policies on other legal issues in its Terms of Service [42].

6 Conclusion

The question remains whether the privacy, security and discoverability risks to wearable health devices such as fitness trackers outweigh the benefits that these wearables can provide. There is a need to balance the privacy and security concerns against the potential improvements that can be made with respect to the health and wellness of consumers, the health care system and society as a whole. Given the as yet unsettled issues with the privacy and security of data from wearable health devices, the clear indication that this data will be requested and admitted as evidence in litigation and the lack of true understanding by users of the risks that these devices may pose, leads the authors to question whether the use of these devices is fitness or folly.

References

1. Ledger, D., McCaffrey, D.: Inside wearables: how the science of human behavior change offers the secret to long-term engagement. Endeavour Partners, LLC (2014). http://endeavourpartners.net/assets/Endeavour-Partners-Wearables-and-the-Science-of-Human-Behavior-Change-Part-1-January-20141.pdf. Accessed 19 Oct 2016
2. Marr, B.: 15 noteworthy facts about wearables in 2016 (2016). http://www.forbes.com/sites/bernardmarr/2016/03/18/15-mind-boggling-facts-about-wearables-in-2016/. Accessed 24 Feb 2017
3. Pricewaterhouse Coopers: The wearable future. In: Consumer Intelligence Series (2014). http://www.pwc.com/us/en/technology/publications/assets/pwc-wearable-tech-design-oct-8th.pdf. Accessed 28 Feb 2017
4. Davenport, T.H., Lucker, J.: Running on data: activity trackers and the Internet of Things. Deloitte Rev. **16**, 5–15 (2015)
5. The Office of the National Coordinator for Health Information Technology: Breaches of unsecured protected health information (2016). https://dashboard.healthit.gov/quickstats/pages/breaches-protected-health-information.php. Accessed 28 Feb 2017
6. EMC Corporation: Cybercrime and the health care industry (2013). http://www.emc.com/collateral/white-papers/h12105-cybercrime-healthcare-industry-rsa-wp.pdf. Accessed 28 Feb 2017
7. Goh, J.P.L.: Privacy, security, and wearable technology. Landslide **8**(2), 30–33 (2015)
8. Hunt, A.: Experts: wearable tech tests our privacy limits. USA Today, 5 February 2015. Available at http://www.usatoday.com/story/tech/2015/02/05/tech-wearables-privacy/22955707/. Accessed 24 Feb 2017

9. Zubulake v. UBS Warburg, 217 F.R.D. 309 (S.D.N.Y. 2003); Zubulake v. UBS Warburg, 216 F.R.D. 280 (S.D.N.Y. 2003); Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2003); Zubulake v. UBS Warburg, 229 F.R.D. 422 (S.D.N.Y. 2004)
10. Federal Rules of Civil Procedure As Amended to December 1, 2016. Available via Legal Information Institute at https://www.law.cornell.edu/rules/frcp. Accessed 8 Feb 2017
11. Fuchs, J.L., McLean, C.G., Fiorentinos, I.S., et al.: Noteworthy trends from cases decided under the recently amended Federal Rules of Civil Procedure (2016). Available via Jones Day at http://www.jonesday.com/noteworthy-trends-from-cases-decided-under-the-recently-amended-federal-rules-of-civil-procedure-09-06-2016/. Accessed 28 Feb 2017
12. Nelson, S.D., Simek, J.W.: The internet of everything: what it means for lawyers (2014). Available via Sensei Enterprises at https://senseient.com/articles/the-internet-of-everything-what-it-means-for-lawyers/. Accessed 28 Feb 2017
13. Gottehrer, G.: "Connected" discovery: what the ubiquity of digital evidence means for lawyers and litigation. Richmond J. Law Technol. **22**, 1–27 (2016)
14. Odendahl, M.: Fitness trackers add to flood of digital evidence in court (2016). Available via The Indiana Lawyer at http://www.theindianalawyer.com/fitness-trackers-add-to-flood-of-digital-evidence-in-courts/PARAMS/article/41112. Accessed 28 Feb 2017
15. Matthews, D.R.: Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval, 2nd edn. CRC Press, Boca Raton (2016)
16. Evenson, K.R., Goto, M.M., Furberg, R.D.: Systematic review of the validity and reliability of consumer-wearable activity trackers. Int. J. Behav. Nutr. Phys. Act. **12**, 159–181 (2015)
17. Weintraub, K.: Wearable health monitors not always reliable, study shows, 12 October 2016. Available via USA Today. http://www.usatoday.com/story/news/2016/10/12/wearable-health-monitors-not-always-reliable-study-shows/91922858/. Accessed 28 Feb 2017
18. Chauriye, N.: Wearable devices as admissible evidence: technology is killing our opportunity to lie. Catholic Univ. J. Law Technol. **24**(2), 495–528 (2016)
19. Hambright, B.: Police: knife, vodka used to stage scene report debunked: crime woman alleged she work up to man assaulting her; officers say Fitbit device conflicted with story. LNP (Lancaster, PA), 20 June 2015, p. 3 (2015)
20. Murphy, P.: Wearables: e-discovery's new frontier? (2015). Available via Rhode Island Lawyers Weekly at http://rilawyersweekly.com/blog/2015/05/14/wearables-e-discoverys-new-frontier/. Accessed 28 Feb 2017
21. Schetzer, A.: Look who's minding your step count. The Sun Herald (Sydney, Australia), 28 December 2014, p. 15 (2014)
22. Kuitenbrouwer, P.: Your fitness tracker could be a snitch. Financial Post, 5 May 2015, p. FP5 (2015)
23. Hitchcock, H.: Who's keeping track of workers' fitness trackers? The Western Mail, 5 August 2015, p. 20 (2015)
24. Hook, S.A.: Real-world examples, handy how-to's and sample screen shots. In: How to Get Your Social Media, Email and Text Evidence Admitted into Evidence (and Keep Theirs Out). National Business Institute, Eau Claire (2016)
25. Brown, E.A.: The Fitbit fault line: two proposals to protect health and fitness data at work. Yale J. Health Policy Law Ethics **16**(1), 1–49 (2016)
26. Fitbit Press Release (2015). https://investor.fitbit.com/press/press-releases/press-release-details/2015/Fitbit-Extends-Corporate-Wellness-Offering-with-HIPAA-Compliant-Capabilities/default.aspx. Accessed 28 Feb 2017

27. U.S. Department of Health and Human Services: HITECH Act Enforcement Interim Final Rule (2009). https://www.hhs.gov/hipaa/for-professionals/special-topics/HITECH-act-enforcement-interim-final-rule/index.html?language=es. Accessed 28 Feb 2017
28. Rockwell, K.L.: The promise of telemedicine: current landscape and future directions. Michigan Bar J. **96**(2), 38–42 (2017)
29. Sullivan, T.: FDA device guidance: general wellness policy for low risk devices (2015). Available via Policy and Medicine at http://www.policymed.com/2015/01/fda-device-guidance-general-wellness-policy-for-low-risk-devices.html. Accessed 28 Feb 2017
30. Spann, S.: Wearable fitness devices: personal health data privacy in Washington State. Seattle Univ. Law Rev. **39**, 1141–1432 (2016)
31. Indiana Code 24-4.9, Sections 1-5: Disclosure of security breach. https://iga.in.gov/legislative/laws/2015/ic/. Accessed 28 Feb 2017
32. Indiana Code 4-1-6, Sections 1-9: Fair information practices; privacy of personal information. https://iga.in.gov/legislative/laws/2015/ic/. Accessed 28 Feb 2017
33. Indiana Code 4-6-14, Sections 1-15: Health records and identifying information. https://iga.in.gov/legislative/laws/2015/ic/. Accessed 28 Feb 2017
34. Nelson, S.D., Ries, D.G., Simek, J.W.: Locked Down: Practical Information Security for Lawyers, 2nd edn. American Bar Association, Chicago (2016)
35. Appendix F. Massachusetts Regulations – Personal Information Protection. In: Nelson, S.D., Ries, D.G., Simek, J.W. (eds.) Locked Down: Practical Information Security for Lawyers, 2nd edn. American Bar Association, Chicago (2016)
36. Medical Records – Health Care Information Access and Disclosure. Available via Washington State Legislature at http://app.leg.wa.gov/RCW/default.aspx?cite=70.02. Accessed 28 Feb 2017
37. Reuhs, N.: Insurance coverage for the Internet of Things. The Indiana Lawyer 27:8 (2017)
38. Könings, B., Schaub, F., Weber, M.: Who, how, and why? Enhancing privacy awareness in ubiquitous computing. In: 2013 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). IEEE, pp. 364–367 (2013)
39. Motti, V.G., Caine, K.: Users' privacy concerns about wearables. In: Brenner, M., Christin, N., Johnson, B., Rohloff, K. (eds.) FC 2015. LNCS, vol. 8976, pp. 231–244. Springer, Heidelberg (2015). doi:10.1007/978-3-662-48051-9_17
40. Let's talk about privacy, publicly. Available via Fitbit at https://www.fitbit.com/legal/privacy. Accessed 27 Feb 2017
41. Privacy Policy. Available via Fitbit at https://www.fitbit.com/legal/privacy-policy. Accessed 27 Feb 2017
42. Terms of Service. Available via Fitbit at https://www.fitbit.com/legal/terms-of-service. Accessed 27 Feb 2017