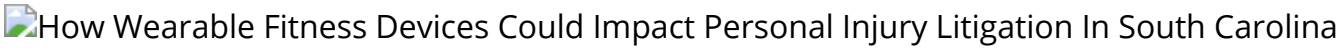

How Wearable Fitness Devices Could Impact Personal Injury Litigation In South Carolina

Laura P. Paton, Sarah E. Wetmore And Clinton T. Magill

Introduction

Wearable fitness devices ("wearables") have become a phenomenon in the United States.1 While health conscious persons used to rely on once-innovative treadmill data, they now rely on smaller, portable devices fashionably strapped to their limbs. However, because they are such simple and personalized products, their impact has gone mainstream and reached a significantly large— yet previously untapped—majority of Americans who simply want to feel rewarded for their personal fitness successes. That is precisely why around 70 million wearable fitness devices—such as Fitbits, Garmins or "smart" devices such as the Apple Watch—were sold in 2014. 2

While consumers are undoubtedly excited about their new fitness toys, they are not alone. Many personal injury litigators are similarly eager to explore the collateral effect of the rising fitness device market: the increasing production of personalized health data. For example, imagine that you are defending a personal injury claim wherein a plaintiff alleges that she is unable to execute essential physical activities and suffers from insomnia as a result of her injuries. While the claimant's allegations may be damning at first blush, her fitness devices may tell a different story. Obtaining contradicting data from those devices may prove very valuable in demonstrating that the alleged injury is not as debilitating as claimed.

The potential value of wearable fitness devices is not restricted to the defense of a personal injury claim. In November 2014, a Canadian plaintiff's attorney made headlines proclaiming that he would use Fitbit data to prove that his client had experienced a decline in physical activity after sustaining an injury in a car accident.3 The lawyer in that case, Simon Muller of McLeod Law LLP, claimed that prior to the injury his client was a personal trainer in "peak physical shape."4 By utilizing Vivametrica, a company that specifically analyzes personal health data, Muller hoped to prove how inactive the former personal trainer had become as a result of the accident.5 Although this is the first well-publicized instance in which a fitness device was used in any legal proceeding, it will likely not be long until personal injury litigants in American courts start asking opposing parties to produce their fitness health data during discovery.6

How the courts will respond to the all-but-certain objections to these requests is not so clear; however, there are several important factors to contemplate when attempting to obtain and use data from wearable fitness devices in litigation. First, from a practical perspective, litigants will need to understand where these devices store data, how the user can access data, and how to ultimately retrieve a

to understand where these devices store data, how they secure data, and how to ultimately retrieve that data. Next, because certain health data is protected, litigants need to be aware of any potential implications under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as well as

the Fourth and Fifth Amendments. Finally, if a litigant is able to get access to the opposing party's fitness data, the next consideration is how to get the data into evidence.

Practical perspective

Fitbit is probably the most well known of the wearable fitness devices, and a look into its privacy policy—which is similar to Garmin's and Apple's—reveals a plethora of information about its data collection and storing procedures. In general, by simply using the Fitbit service, consumers consent to allowing it to process the health and fitness data it collects in accordance with its privacy policy. 7 The policy asserts that while Fitbit promises to provide users with immediate access to their health and fitness data, it also promises to respect users' privacy and to keep their data both safe and secure.8 To activate a device and make personalized data accessible, users must create a Fitbit account on its websites, its mobile application, or both.9 In doing so, users provide Fitbit with some initial personal information such as height, weight, gender, date of birth and e-mail address.10 The devices may then transmit collected data and other statistics to Fitbit, including number of steps taken, weight, sleep quality, calories burned or distance traveled.11 Importantly, once a user syncs his or her device, data recorded about a user's activity is automatically transferred from the device to the Fitbit servers.12 This data is then stored by Fitbit and is associated with a user's account in order to provide the Fitbit service.13 This raises the question as to how to obtain that health data.

Generally, Fitbit claims to only share a user's data "when it is necessary to provide the Fitbit service, when the data is de-identified and aggregated, or when [the user] direct[s] us to share it."14 For example, a user may request that Fitbit share his or her data with an employer pursuant to an employee wellness program.15 However, where a party refuses to share its information, Fitbit can still provide the data if "disclosure is reasonably necessary to comply with a law, regulation, valid legal process (e.g., subpoenas or warrants served on us), or governmental or regulatory request."16 Therefore, if a user is not willing to direct Fitbit to share his or her data, a court order or subpoena will likely be necessary.

Obviously, if a user is unwilling to share his data, litigants will face some procedural obstacles. This could be especially worrisome in cases where a party may attempt to destroy her personal fitness data. Normally, Fitbit stores a user's personalized data for as long as the user maintains a Fitbit account.17 However, users are able to modify or delete certain data.18 The upside is that, even when a user removes data from his or her Fitbit account, "backups of that data will remain associated with [the user's] Fitbit account and in [Fitbit's] archive servers."19 Copies of this backup data are removed pursuant to an automated schedule, so data may potentially remain in Fitbit's archives only for a short period of time.20 Accordingly, a fastacting litigant may be able to protect and save an opposing party's deleted fitness data if he sends a "litigation hold" letter to Fitbit and the claimant and quickly follows up by pursuing the appropriate discovery, court order or subpoena on the company collecting the data.

HIPAA considerations

HIPAA provides both privacy and security standards that are applicable to certain entities. While this article does not explore all aspects of HIPAA or other state and federal privacy protections that may

be implicated, some broad considerations are discussed herein. The Standards for Privacy of Individually Identifiable Health Information ("the Privacy Rule") of HIPAA aim to assure that an individual's health-related data is adequately protected while simultaneously permitting the flow of health data needed to promote and provide top-notch health care and protect the public's well-being.21 Similarly, the Security Standards for the Protection of Electronic Protected Health Information ("the Security Rule") aim to protect an individual's private health data while simultaneously permitting covered entities to implement new technology to improve both the efficiency and quality of patient care.22 However, the simple fact that data specifically relates to health does not make it subject to HIPAA restrictions. Instead, the key questions to consider are 1) who has possession of the data and 2) what are they doing with that information.

HIPAA generally imposes duties on certain "covered entities" that possess, use and transmit private health information. Thus, a wearable fitness device owner does not have any obligation to secure the information. Accordingly, users are free to share—or not share—their data with whomever they please. So where do wearable fitness data companies fall in this equation? Covered entities under HIPAA are health plans, health care clearinghouses or health care providers that transmit health data in connection with certain transactions in an electronic form. Fitbit and other companies like it are probably not covered entities, because they neither provide health care nor pay for health care, and because they can neither be considered a health plan nor a health care provider. Similarly, they are not health care clearinghouses, as those entities are typically intermediaries between health care providers and insurers that process nonstandard information they receive from another entity into a standard format.

Although these companies do not fall into one of the general "covered entity" categories, the Health Information Technology for Economic and Clinical Health Act ("the HI-TECH Act") extended compliance with the Privacy Rule to business associates of covered entities. Thus, Fitbit or similar companies could be considered business associates if they convey information to health insurers. For example, some insurance plan companies offer to their insureds the option to gather information from Fitbit to track their insured's health in exchange for premium reductions or other rewards.23 If Fitbit shares that information with the insurance plan, it may become a business associate and therefore be bound by both the Privacy and Security Rules. There may even be business associate agreements in place that cover this, including indemnification agreements.

If personal fitness device companies are bound by the Privacy Rule, they must abide by several standards regarding the disclosure of private health information. Under the Privacy Rule, a covered entity—and by the HI-TECH Act extension, its business associates— may only disclose personal health information to another party pursuant to an enumerated exception or with an authorization, notice and an opportunity to object, or by court order. As stated in its privacy policy, simply using the Fitbit service authorizes Fitbit to utilize a user's data in accordance with its privacy policy. Accordingly, whether HIPAA applies may not matter—as a court order is likely sufficient to authorize the disclosure of a user's information.24

The savvy attorney in a new case where an alleged personal injury is at issue should consider a few precautionary steps. First, regardless of whether a claimant uses a personal fitness device, counsel should immediately send correspondence regarding protection and maintenance of any potential wearable fitness data to opposing counsel followed by written discovery requests regarding the identity of any wearables utilized and production of data stored on the device. Once information as

to the wearable company is received, counsel should review the wearable company's policies and send a "litigation hold" letter to the wearable company and opposing counsel to maintain the information in their files. Finally, depending on the terms of the wearable company's privacy policy

and the position of the claimant, if appropriate, counsel should consider preparing a HIPAA waiver request and subpoena the information from the wearable fitness device company. Tread lightly, however, as there are various state and federal rules and regulations implicated including Rules 34 and 37, SCRCP, and the Electronic Communications Privacy Act.25

Using Fitbit data at trial

The ultimate question is how parties to personal injury litigation could use personal fitness data as evidence at trial. In the Canadian lawsuit, Simon Muller explained that while medical opinions were provided and lawyers had their chances to ask questions, Fitbit data would be used simply to boost his client's case. Importantly, however, Muller did not offer the raw data as direct evidence. Data from personal fitness devices is likely not admissible as direct evidence. Under South Carolina Rule of Evidence 402, relevant evidence is generally admissible. Accordingly, in personal injury cases data from wearables would certainly be relevant under Rule 401 as it would have a tendency to make the existence of a fact—for example, the extent of a claimed injury—more probable or less probable than it would be without the data. Nonetheless, litigants would also have to authenticate this data as reliable pursuant to Rule 901 SCRE, demonstrate that the data passes muster under 702 SCRE, and respond to hearsay objections under Rule 802. All of this is likely problematic because a party opposing admissibility may argue as to the unreliability and inaccuracy of the device. Furthermore, a litigant would have trouble proving that the user did not modify the data or that the data produced by the device was actually produced when the other party was wearing it—as opposed to a family member or spouse. Finally, there may be Fifth Amendment or other constitutional challenges to the admission of this data. Notwithstanding, wearable data may be admissible if used to prove that an allegedly injured party was active before an accident or as a statement of the declarant's then-existing physical condition under Rule 803(3), SCRE.

The most likely way of getting wearable data before a jury is to have a qualified expert review it and rely upon it as the basis of her opinion. Under South Carolina Rule of Evidence 703, an expert need not rely only on data that is admissible. Thus, it is possible that an expert could testify that she relied on wearable data in forming her opinions, and the jury would then determine the reliability and weight of the evidence. That expert's opinion may be subject to attack and not given much weight because data from wearable fitness devices is probably not reasonably relied upon by other experts in the field when forming their opinions or inferences.

Conclusion

With the emergence of the wearable fitness device market comes an increase in personalized health and fitness data for discovery and investigation. In personal injury litigation, this data could be invaluable to a party's case. How the courts will ultimately respond to attempts to introduce this data in litigation remains unclear. A basic understanding of the data that these devices collect—and how to ultimately retrieve it—is vital to the litigant's efforts. While HIPAA protections are unlikely to apply to personal fitness devices in general, they could be implicated where fitness device companies contract with health care providers or health plans as business associates. However, even where HIPAA protections do not apply, litigants could face multiple hurdles in their mission to rely on personalized fitness data at trial. Regardless, the debate over personal fitness data has just

rely on personalized fitness data at trial. Regardless, the debate over personal fitness data has just begun—and the impending battle between relevance and reliability will have a significant impact on personal injury litigation in the South Carolina courts for years to come.

Laura Paton is of counsel and Sarah Wetmore is a partner in the Charleston office of Carlock, Copeland & Stair, LLP. Clinton T. Magill is in his third year at the Charleston School of Law.

Endnotes

1 Jo Craven McGinty, Fit for Motivation if Not Precision, The Wall Street Journal (Jan. 9, 2015, 7:07 p.m.), www.wsj.com/articles/ wearable-fitness-gadgets-fall-short-onaccuracy- but-theyre-good-cheerleaders- 1420820247 (citing to an NPD market research study finding that 1 in 10 Americans uses a wearable fitness device)

2 Nick Statt, The Rise and Fall of Fitness Trackers, CNET, (Jan. 1, 2015, 5:00 a.m.), www.cnet.com/news/fitness-trackers-riseand- fall/.

3 Jennifer Brown, Data Fit for the Courtroom?, CANADIANLAWYER, (Feb. 2, 2015), www.canadianlawyermag.com/5450/ Data-fit-for-the-courtroom.html.

4 Id.

5 Id.

6 See Mariella Moon, Fitbit Tracking Data Comes Up in Another Court Case, ENGADGET, (June 28, 2015), www.engadget.com/2015/ 06/28/fitbit-data-used-by-police.

7 Privacy Policy, Fitbit www.fitbit.com/privacy (last visited Aug. 10, 2015).

8 Id.

9 Id.

10 Id.

11 Id; see also Compare, Fitbit www.fitbit.com/ compare (last visited Aug. 10, 2015) (for a more exhaustive list of what type of data that each Fitbit device collects).

12 Privacy, supra note vii.

13 Id.

14 Id.

15 Id.

16 Id.

17 Id.

18 Id.

19 Id.

20 Id.

21 45 C.F.R. §§ 160, 164(A), (E) (2002).

22 45 C.F.R. 160, 164(A), (C) (2003).

23 HUMANA VITALITY, www.humana.com/learning-center/health-and-wellbeing/fitness-and-exercise/devices

24 At the time of writing, the authors have not found any published rulings on this issue, but given the ubiquitous use of these devices, the authors believe that this issue will likely be tested in the near future.

25 18 U.S.C. § 2702(c)(6) (2012). See also Matthew R. Langley, Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables, 103 Geo. L.J. 1641, 1650 (2015).