Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Wearable Fitness Devices: A New Frontier In Discovery

Law360, New York (March 28, 2016, 10:10 AM ET) --
Wearable fitness devices (commonly referred to as "wearables") constitute one of the latest trends in technology, and likely represent a new frontier in discovery disputes. These devices are exactly what they sound like — functional electronic wristbands designed to monitor and record an individual's daily fitness activity.[1] Unlike handheld devices, wearables can monitor and record physical activity and sensitive health information — such as a user's heartrate, skin temperature, or respiratory rate — in real time.[2] Additionally, as stated on one wearable's website, they are able to track "every part of [the user's] day — including activity, exercise, food, weight and sleep.[3]"


Carol Michel


Rick Sager

As these devices become more and more popular (recent studies show that roughly one in five U.S. consumers own a wearable device),[4] it is highly likely that these devices will become a common part of litigation disputes. The opportunities for use in the courtroom are abundant. The data recorded and stored by these devices has the potential to bolster or dispute any claim related to personal injury, or any other time a person's health information is relevant to a claim or defense. Wearables collect and store a user's personal health information 24 hours a day, seven days a week. They are the functional equivalent of a "black box" for the human body.

Of course, with this new technology comes a variety of concerns as to how this information can be utilized in the courtroom, ranging from collectability of such data in discovery, to admissibility at trial. This article will discuss relevant issues to be aware of as this area of litigation develops.

Examples of Wearables Data Used in a Legal Proceeding

The first well-publicized use of a fitness device in a legal proceeding took place in Canada in November 2014.[5] The plaintiff in this case used the data from her wearable fitness device to prove that she had experienced a decline in physical activity after sustaining an injury in a car accident.[6]

In March of 2015, police from Lancaster, Pennsylvania, used data from a wearable fitness device to support charges of false report to law enforcement, false alarms to public safety, and tampering with evidence.[7] The police used evidence from the defendant's wearable fitness device to contradict a

statement made by the defendant.[8] During the time that the defendant alleged that she was sleeping, her wearable fitness tracker showed that she was awake and active.[9] The police used this information to bolster their claim that this was the time that she was staging a fake crime scene.[10]

Collectability issues

Although wearable fitness devices generate vast amounts of data that would be useful in litigation, notable issues may arise related to the discovery and collectability of this data. While we do not currently have many real-life examples related to how courts will handle a dispute involving the disclosure of data from a party's wearable fitness device, there are practical considerations that may provide guidance as to how this process may play out.

As a preliminary matter, the information from an individual's wearable fitness device may be public, and formal discovery may not even be required. If an individual has elected to keep most, if not all, of their profile related to their fitness device publicly viewable, an abundance of information may be available. As such, "informal discovery" (hello, Google) may be a viable option.[11] If their profile is private, then more formal discovery efforts will be necessary.

One issue that may arise is the question of who actually owns the data in the first place — the user or the provider.[12] For example, the privacy policy of one manufacturer of wearables pledges that they will "let [the user] decide how [their] information is shared."[13] This same policy offers a significant exception, however, asserting that even when a party refuses to share their information, the corporation 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 requests."[14]

Similar discovery disputes have arisen in the context of social media, debating "whether the discovery request should be directed to the social networking site directly or to the party whose information is being sought."[15] It is yet to be determined what challenges may arise if a party asks the court to serve a subpoena on a provider of a wearable fitness device. Whether the information recorded by the wearable fitness device is within the control, possession or custody of the person who posted it, and to what degree a threshold showing of relevance is required from the party seeking discovery, are all considerations that could be a factor.[16]

Another scenario is one in which a party seeks to compel the disclosure of the user's wearable fitness device password and login credentials. Again, this is an area of discovery that has been hotly contested in the context of social media. As expected, courts have been all across the board — ranging from "upholding the production of social media passwords to those that reject such unlimited access, as well as the courts that take a "middle ground" approach and allow complete access upon satisfaction of some other threshold requirement or that such access will be predicated upon an in camera review."[17] A key defense utilized by parties involved in discovery disputes — that of privacy — may be lost in the context of wearables. Unlike social media in which the very nature of use is to broadcast information, wearable fitness devices are more personal and have a utilitarian purpose of helping the user keep track of their health (although, the temptation to boast about one's six-mile morning run may be too much to bear, and may render this point moot).

One last matter to consider is that time may be of the essence when it comes to collecting information from a user's wearable fitness device. There is nothing that prevents a user from modifying or deleting his or her information from their device. For this reason, a timely hold letter is likely the most

practicable course of action in order to ensure that this information is not lost.[18] Further, even if the user is able to delete their information, most providers of wearable fitness devices maintain backups of this data that is stored in the provider's archives for a short amount of time.[19] This may be a situation where the prudent course of action would be to have the court issue a subpoena to the provider to preserve the information until the litigation has been resolved.

HIPAA and the SCA

The Health Insurance Portability and Accountability Act, a landmark 1996 patient-privacy law, covers patient information kept by health providers, insurers and data clearinghouses, and their business partners.[20] The purpose of this act is to make sure that an individual's health-related data is kept secure while simultaneously allowing these "covered entities" to possess, use, and transmit private health information in order to provide the best quality health care to patients.

Wearable technologies companies, like Fitbit or the Apple Watch, do not fall within the confines of "health providers, insurers and data clearinghouses, and their business partners," and thus are not covered by HIPAA protections.[21] Therefore, even though these devices stores vast amounts of health-related data, the fact that their data relates to health does not make it subject to HIPAA restrictions.

The Stored Communications Act is another way in which Congress sought to provide appropriate privacy protections for the growing trend of Internet activity.[22] Section 2703 of this act provides the rules that the government must follow in order to compel a provider to disclose information about its customers involuntarily.[23] With regard to the content of communications, the government must obtain a search warrant, subpoena, or "2703(d) order" to compel disclosure of the information. With respect to noncontent records, the government can compel disclosure through a warrant, a 2703(d) order, consent of the customer, or by submitting a written request to the provider.[24] In its current form, the SCA treats personal health data obtained through wearable fitness devices as noncontent records. Thus, the SCA provides almost no protection for individuals using wearables.

As such, data recorded from wearable fitness devices seems to fall into no-man's land with regard to HIPAA and the SCA. While wearable technology deals with health-related data, this in and of itself does not qualify this data for the protections afforded under the Health Insurance Portability and Accountability Act. Further, while these devices record data that is similar to the communications that the SCA was drafted to protect, the data recorded by these devices is considered to be a non-content record, rather than a communication. Current legislation is one more factor that may be necessary to consider when seeking to recover data recorded from wearable fitness devices to use in litigation.

Using the Information at Trial

Ultimately, questions will still arise as to how parties to litigation can use data from a wearable fitness device at trial. Depending on the nature of the litigation, the first barrier to admission at trial would be whether the information is relevant. Of course, "relevant evidence" means evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.[25] While the issue of relevance may be an easy hurdle to clear (particularly in a personal injury claim or any other time a person's health information is relevant to a claim or defense), litigants will also have to overcome basic reliability concerns, and that the effectiveness of wearable data is dependent on its interpretation and application by a properly qualified individual.[26]

Opponents will raise every defense imaginable — hearsay objections, the inaccuracy or unreliability of the device, authentication concerns, proving that the individual actually wore the device rather than a friend or relative, or constitutional challenges. All of this is up to speculation. One scholar has suggested that the best way to get the wearable data before the jury is to have a qualified expert review it and rely upon it as the basis of her opinion.[27] Under Federal Rule of Evidence 703, an expert does not need to rely on evidence that is admissible. Therefore, an expert could potentially "testify that she relied upon wearable data in forming her opinions, and the jury would then determine the reliability and weight of the evidence."[28] This may be subject to attack, however, because the "data from wearable fitness devices may not be reasonably relied upon by other experts in the field when forming their opinions or inferences."[29] It may be that an adequate foundation can be laid by using the manufacturer's own accuracy data to establish the bona fide's of the device sufficient for an expert to rely upon its data.

Conclusion

There is no question that wearable fitness devices are a developing phenomenon in the United States. The personal health data that is recorded and stored from these devices is a veritable goldmine of information for parties to litigation. While there have not been any major decisions on the applicability of this information in the courtroom, it is only a matter of time before parties will seek to introduce this information at trial. A general awareness of collectability and discovery concerns, along with an understanding of HIPAA, the SCA and other legislation could pay dividends down the road in seeking to utilize this valuable information in a trial.

—By Carol Michel and Rick Sager, Weinberg Wheeler Hudgins Gunn & Dial LLC

Carol Michel is a partner in Weinberg Wheeler's Atlanta and Las Vegas offices. Rick Sager is a partner in the firm's Atlanta office.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] See Matthew R. Langley, Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables, 103 Geo. L.J. 1641, 1643 (2015) (providing a general description of wearable technology); See also Kiana Tehrani & Andrew Michael, Wearable Technology and Wearable Devices: Everything You Need to Know, WEARABLE DEVICES MAG. (last updated Mar. 26, 2014), http://www.wearabledevices.com/what-is-a-wearable-device/ (providing a basic overview on what constitutes a wearable device).

[2] Langley, supra note 1, at 1644; See also David Pogue, Wearable Devices Nudge You to Health, N.Y. Times, June 26, 2013, http://www.nytimes.com/2013/06/27/technology/personaltech/wearable-devices-nudge-you-to-a-healthier-lifestyle.html?_r=0 (describing various wearable devices and their basic functions).

[3] Fitbit, https://www.fitbit.com/whyfitbit (last visited Jan. 20, 2016).

[4] Langley, supra note 1, at 1645.

[5] See Kate Crawford, When Fitbit Is the Expert Witness, The Atlantic (Nov. 19, 2014), http://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/ (discussing the legal proceeding in Canada that utilized information from wearable technology).

[6] Id.

[7] Myles Snyder, Police: Woman's Fitness Watch Disproved Rape Report, ABC27, June 19, 2015, http://abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/.

[8] Id.

[9] Id.

[10]Id.

[11] See John G. Browning, Digging for the Digital Dirt: Discovery and Use of Evidence from Social Media Sites, 14 SMU Sci. & Tech. L. Rev. 465, 471 (2011) (discussing informal discovery techniques within the context of social media profiles. While this article discusses how informal discovery techniques can be used related to social media, similar techniques can also be employed for public profiles of users of wearable fitness devices).

[12] Neda Shakoori, Wearables: Your Next Trial Witness?, S.F. Daily Journal, Dec. 10,2014. San Francisco Daily Journal.

[13] Privacy Policy, Fitbit www.fitbit.com/privacy (last visited Jan. 20, 2016).

[14] Id.

[15] John G. Browning, With "Friends" Like These, Who Needs Enemies? Passwords, Privacy, and the Discovery of Social Media Content, 36 Am. J. Trial Advoc. 505, 508 (2013).

[16] Id.

[17] Id. at 508-09.

[18] See Laura P. Paton, Sarah E. Wetmore, Clinton T. Magill, How Wearable Fitness Devices Could Impact Personal Injury Litigation in South Carolina, 27 S.C. Law. 44, 47 (2016) (noting that a "fast-acting litigant may be able to protect and save an opposing party's deleted fitness data if he sends a 'litigation hold' letter to [the provider] and the claimant quickly follows up by pursuing the appropriate discovery, court order or subpoena on the company collecting the data.").

[19] See id. (discussing Fitbit's policy of storing backups of data that will remain associated with a user's Fitbit account and in Fitbit's archive servers).

[20]See generally Health Insurance Portability and Accountability Act, PL 104–191, August 21, 1996, 110 Stat 1936.

[21] See Charles Ornstein, Federal Privacy Law Lags Far Behind Personal-health Technologies, Wash. Post, Nov. 17, 2015, https://www.washingtonpost.com/news/to-your-health/wp/2015/11/17/federal-privacy-law-lags-far-behind-personal-health-technologies/. (discussing the fact that wearables, like Fitbit, fall outside HIPPA's purview).

[22] See Matthew R. Langley, Hide Your Health: Addressing the New Privacy Problem of Consumer Wearables, 103 Geo. L.J. 1641, 1652 (2015) (providing a general overview of the SCA).

[23] 18 U.S.C. § 2703 (2012); see also Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1219 (2004) (discussing the rules that the government must follow in order to compel a provider to disclose information about its customers.).

[24] Langley, supra note 1, at 1652 (2015).

[25] Fed. R. Evid. 401

[26] See John Faubion, Could Fitbits Become Expert Witnesses in the Courtroom?, Cooper & Scully, PC, http://www.cooperscully.com/news-and-resources/articles/could-fitbits-become-expert-witnesses-in-the-courtroom (last visited Jan. 20, 2016) (discussing various obstacles parties may face in seeking to use data from wearable devices in litigation).

[27] See Laura P. Paton, Sarah E. Wetmore, Clinton T. Magill, How Wearable Fitness Devices Could Impact Personal Injury Litigation in South Carolina, 27 S.C. Law. 44, 48 (2016) ("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.").

[28] Id.

[29] Id.

All Content © 2003-2016, Portfolio Media, Inc.