IADC COMMITTEE NEWSLETTER

TECHNOLOGY

July 2015

IN THIS ISSUE

This article examines a new frontier in electronic evidence: the use of data from activity fitness trackers, such as Fitbit or Jawbone, as evidence to support or disprove a party's claims or defenses. As the article demonstrates, this new source of evidence is already being used in both civil and criminal cases, and is likely to appear frequently as the wearable technology trend continues.

Fitbit Data Brings Another Dimension to Evidence

ABOUT THE AUTHOR

John G. Browning is a Shareholder at Passman & Jones, where he handles civil litigation in state and federal courts, in areas ranging from employment and intellectual property to commercial cases and defense of products liability, professional liability, media law, and general negligence matters. Mr. Browning has extensive trial, arbitration, and summary judgment experience and has represented companies in a wide variety of industries throughout Texas. He is also a Charter Fellow in Litigation Counsel of America. He is the author of the books *The Lawyer's Guide to Social Networking, Understanding Social Media's Impact on the Law*, (West 2010), the *Social Media and Litigation Practice Guide* (West 2014); and *Cases & Materials on Social Media and the Law* (forthcoming, Carolina Academic Press). An award-winning author, Mr. Browning has published hundreds of articles for practitioners and the public, as well as more than twenty-five academic articles. He can be reached at browningj@passmanjones.com.

ABOUT THE COMMITTEE

The Technology Committee keeps the IADC membership current on the use of technology in litigation, whether in the conduct of discovery or in the use of technology in the courtroom. It educates its members on the impact of technology in their practices – on the ways they communicate with each other, with courts and clients, on the systems they use to record and produce their work, and on technological developments in marketing for law firms. The committee provides information to its members on legal developments in the law governing the use and development of technology, in particular on Internet and computer law and related subjects. Through its members, it acts as a resource to the IADC staff and leadership on technology issues facing the organization. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Peter J. Pizzi
Vice Chair of Publications
Connell Foley LLP
ppizzi@connellfoley.com

On Monday, John Smith posted the stats of his morning run to Facebook via an app called Runkeeper, while the Fitbit wristband he wore dutifully tracked the number of steps he took and the calories he burned. And on Tuesday, the lawyer representing Mr. Smith in a personal injury lawsuit called Smith to say he'd received discovery requests seeking "all data gathered and stored by fitness tracking devices and/or other forms of wearable technology reflecting John Smith's physical activity levels since the date of the accident made the basis of suit."

Farfetched? Hardly. From Google Glass to Apple's smartwatch, wearable technology has arrived in a big way. The Gartner research firm estimates that the $1.6 billion wearable technology field will generate $5 billion in revenue by 2016. Activity trackers like Fitbit, Nike Fuelband, and Jawbone UP monitor a whole host of data about one's physical condition, location, exertion level, and vital signs like heart rate; some, like Garmin's Vivosmart, even measure one's sleep. Such wearable devices constitute a veritable "black box" for the human body, using wireless technology to measure movements and synchronize with smartphones and computers to provide users with a wealth of information to keep track of their health. But, this digital treasure trove of insight into the health and lifestyle of the device's wearer can also have considerable value for enterprising attorneys in virtually any kind of case in which an individual's physical condition might be relevant – including not just personal injury cases, but workers compensation claims, employment discrimination litigation, family law matters, and even trade secret lawsuits.

Last November, a Canadian personal injury lawsuit may have helped usher in a new era of wearable technology as a source of evidence. Representing a personal trainer who was injured in an auto accident four years previously, Simon Muller of the McLeod Law Firm in Calgary wanted to show the effects of the accident on his client. Processing the data from her Fitbit, he believed, would enable him to buttress her testimony that her post – injury activity levels were below the norm for someone of her age and profession. "[Until] now we've always had to rely on clinical interpretation," Muller says. "Now we're looking at longer periods of time through the course of a day, and we have hard data."[1] (Parmy Olson, "Fitbit Data Now Being Used in the Courtroom," Forbes.com (Nov. 16, 2014), http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury) Muller didn't just rely on the raw data itself. Instead, he used analytics company Vivametrica to analyze and compare the plaintiff's information with the wealth of data on the general population to demonstrate that her readings were below average, compromised as a result of her injuries.

Yet, Muller's case and the novel questions it raises may not be as groundbreaking as it seems. Here in the United States, social networking apps like Strava with geolocation features and "personal best" times for cyclist users have been used as evidence in civil cases involving biking accidents. And an earlier Canadian case may have helped pave the way for the evidentiary use of personal activity data. In the 2014 case of Laushway v. Messervey, the Nova Scotia Court of Appeals had to weigh the privacy claims of a personal injury plaintiff against the discoverability of electronically stored information that was a window into that plaintiff's activity level.[2] (2014 NSCA 7) Laushway, who prior to his injury ran an internet-based business from his home, claimed that as a result of his injury he could no longer sit at his computer for extended periods of time and had difficulty with other sedentary tasks. The skeptical defense attorneys sought production of metadata stored on the plaintiff's computer hard drive which would reveal when and for how long the plaintiff was actually sitting at and using his computer. Laushway appealed the court's granting of this motion, characterizing it as a fishing expedition that constituted an unreasonable invasion of privacy. The appellate court disagreed, reasoning that this metadata was electronic information that would be accurate, reliable and relevant to Laushway's claims of being unable to work. As for privacy considerations, the court held that there was little privacy interest in metadata that simply showed when and for how long the plaintiff was sitting at a computer. However, the court did narrowly tailor the discovery order, denying the defense unfettered access to all of the plaintiff's stored electronic files and the internet sites he visited.

Even more recently, Fitbit data played a game–changing role in another case. In March 2015, 43 year-old Jeannine Risley of St. Petersburg, Florida was in Lancaster, Pennsylvania for work and staying in a guest room at the home of her boss in East Lampeter Township. On the night of March 10, she reported to authorities that an unknown assailant had pulled her out of bed, struck her in a bathroom and raped her at knifepoint. According to Risley, her fitness tracker was lost in the struggle. But police found the device, and even before they began to analyze it certain elements of Risley's story weren't adding up. For one thing, despite the fact that the house was surrounded in snow, there were no footprints, nor were there any signs of forced entry or an intruder inside the home. Moreover, Risley's employment had recently changed. Prior to the alleged assault, her boss had informed her she would no longer be a temporary director with the company, and instructed her to inform her staff about the change – but she hadn't done so. Finally, although Risley had cooperated with police by providing her username and password for the activity tracker, the device's dongle (the hardware that connects the device to a

computer so that it can be read) was missing from an envelope Risley mailed to police from Florida (her husband later mentioned that it must have been lost in the mail).

The police, however, were undaunted. After downloading her fitness activity on the night in question, it revealed that she had been awake and walking around the entire night – not sleeping as she had claimed. Combined with other evidence that cast doubt on her story, police charged her with making a false report to law enforcement, making a false 911 call, and tampering with evidence. Was this a case of a disgruntled employee seeking payback from her employer by manufacturing a claim that she had been raped by an intruder at his home? We may never know the whole story, but we do know that her activity tracker played a key, if unintended, role in undermining her claims.[3] (Myles Snyder, "Police: Woman's Fitness Watch Disproved Rape Report," ABC News, June 19, 2015; http://www.abc27.com/2015/06/19/police-womans-fitness-watch-disproved-rape-report/)

Given cases like Laushway and especially the Fitbit case argued by attorney Muller, as well as the growing wealth of biometric information being gathered and analyzed by wearable technology, attorneys practicing in the Digital Age must be prepared for the discoverability and admissibility issues that can arise from data from activity trackers like Fitbit. One obstacle is that they lack a uniform standard. Jawbone UP, Fitbit, and Nike Fuelband all have differences in how they work: some count moving your arms around as walking while some have difficulty registering an activity like cycling. Moreover, many devices feature disclaimers urging that data from them, such as heart rate or dehydration level, shouldn't be substituted for an actual medical diagnosis – raising further questions about their reliability. In addition, as with any source of electronically stored information, there's the ever–present danger of hacking or even spoofing (such as having someone else wear the wearable technology). As a result, the data collected by devices like Fitbit or Jawbone may not only have uniformity and reliability problems, but may be subject to manipulation as well.

In light of such concerns, it may be advisable to have a third party service or expert collect and analyze the data (much like Muller's use of Vivametrica) rather than to rely solely on raw data. After all, under Federal Rule of Evidence 703, an expert can base his or her opinion even on inadmissible evidence. But gathering and using personal health data like heart rate and blood pressure also raises privacy issues, since as one legal commentator has pointed out about devices like Fitbit, "Every bit of data that is entered is potentially discoverable if it even becomes relevant to a legal dispute."[4] (Kris Klein, "Fitbit and litigant privacy" www.privacyscan.ca/.../november-28-2014-fitbit-and-litigant-privacy) In Muller's case,

it was the plaintiff herself using the data to support her claims, but what about when evidence from wearable technology is being sought in discovery? It would seem logical that privacy concerns would take a backseat where the information is relevant to claims or defenses in a lawsuit, especially a lawsuit in which the plaintiff herself has put her physical condition in issue, such as a personal injury case.

Assuming that such data can be obtained in discovery, will it be admissible? Judge Paul Grimm of the U.S. District Court for the District of Maryland has been a leading authority on admissibility of electronically stored information, having authored one of the seminal decisions on the subject, Lorraine v. Markel Am. Ins. Co.[5] (241 F.R.D. 534 (D. Md. 2007))

As he pointed out in an article considering the admissibility of social media content "A trial judge should admit the evidence if there is plausible evidence of authenticity produced by the proponent of the evidence and only speculation and conjecture - not facts - by the opponent of the evidence about how, or by whom, it "might" have been created."[6] (How Paul W. Grimm, Lisa Bergstrom, and Melissa O'Toole Loureiro, "Authentication of Social Media Evidence," 36 American Journal of Trial Advocacy 433, 459 (Spring 2013)) There are multiple avenues available pursuant to Federal Rule of Evidence 901 (b) for authenticating ESI from wearable technology like a Fitbit. Rule 901 (b) (1) allows a witness with personal knowledge to authenticate evidence. Just as the author of a Facebook status update might be asked if he created the post, the owner/wearer of a Fitbit can be questioned about her use of the device over a relevant time period, settings that she administered, and the resulting data. One might also incorporate the support of FRE 901 (b) (4), which involves authenticating through distinctive circumstances or characteristics. For example, there may be content unique to the user of the device – references to a particular fitness goal like an upcoming race, nicknames, abbreviations, slang, an internet address, or any other content or factors uniquely tying a particular individual to the data in question. Finally, FRE 901 (b) (3) provides for authentication through the use of an expert, such as a computer forensics expert. Having a qualified expert testify about the data and any pertinent analysis may also involve FRE 901 (b) (9) which deals with a system or process producing reliable results.

Data from wearable devices like Fitbit is already being gathered for purposes beyond just individual monitoring of fitness goals. Some health insurers are offering customers discounts based on data from Fitbit or other activity monitors. So it's hardly surprising that such examples of wearable technology would eventually find their way into the courtroom. The potential legal applications and risks attendant with wearable technology have been the subject of much

discussion.[7] (See, for example, John G. Browning, "Wearable Tech," Texas Bar Journal (January 2015)) Use of devices like Fitbit and others in litigation is likely to gather momentum as time marches on, making it necessary for lawyers to have an understanding of both the benefits and risks associated with their use. And given the reliability issues and limitations on activity tracking technology, perhaps it's wise for device users and lawyers alike to heed the advice of one observer who cautioned that wearables should be thought of "as partial witnesses, ones that carry their own affordances and biases."[8] (Kate Crawford, "When Fitbit Is the Expert Witness," The Atlantic (November 2014), http://www.theatlantic.com/technology/print/2014/u/when-fitbit-is-the-expert-witness)

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

DECEMBER 2014
The Ethics of Technology in E-Discovery – An Introduction
Peter J. Pizzi and Julia L. Brickell

SEPTEMBER 2013
Emerging Technology and Its Impact on Automotive Litigation
John G. Browning

JUNE 2012
iPad Apps: Brave New Frontier
Adam Bloomberg and J. Calhoun Watson

AUGUST 2011
TrialDirector: Electronic Trial Presentation – A Primer, Best Practice Tips
Thomas G. Oakes

MAY 2010
Know When to Hold 'Em: The Effective Use of Litigation Holds
Mike Taylor

JULY 2009
New Insights for Jury Profiling and Online Socialization
Merrie Jo Pitera and Stephanie S. Cox

APRIL 2008
Irish Supreme Court "Creates" E-Discovery: The Disappearing Line between Digital Data and Paper Documents
Robert C. Manlowe, Gregory D. Shelton, and Manish Borde

FEBRUARY 2008
Qualcomm v. Broadcom: Lessons for Counsel and a Road Map to e-Discovery Preparedness
Gregory D. Shelton

JANUARY 2008
Simonetta v. Viad Corp: A Disturbing Expansion of the Duty to Warn in Products Liability Cases
Gregory D. Shelton

MAY 2007
Are You Competent?: Providing Representation in the Digital Age
Gregory D. Shelton

FEBRUARY 2007
Are You Prepared for Litigation Under the New E-Discovery Amendments to the Federal Rules of Civil Procedure?
Gregory D. Shelton and Robert C. Manlowe