WARD AND SMITH, P.A.
ATTORNEYS AT LAW

Activity Tracker Data: Can Your Step Count Be the Key to Winning or Losing a Lawsuit?

December 9, 2016

In 2015, the Fitbit was one of the most popular holiday gifts ordered on Amazon. With the holidays fast approaching, activity trackers such as Fitbit®, Jawbone®, Garmin®, and the Apple Watch® will be popular holiday gifts again. While these activity trackers may be the ideal gift for friends and family hoping to improve their health and wellness in the upcoming year, the legal consequences of wearing these trackers are just starting to develop, and they aren't products liability issues as seen with self-combusting hoverboards or the all too famous "official Red Ryder, carbine action, two-hundred shot range model air rifle" from A Christmas Story that may "shoot your eye out."

Rather, the legal concern for wearers of activity trackers is how the information collected and stored by these devices may be used if a wearer is involved in civil litigation or a criminal prosecution. These devices are designed to, and do track, a wearer's steps and hours of sleep per day, heart rate, and general activity patterns and perhaps even store information about the wearer's location during activity. Indeed, activity trackers are frequently worn 24/7 making them a constant source of a wearer's personal, and once thought to be private, information. The collection of this data presents a whole new realm of evidence that may be used in court. Consider the following four scenarios:

Scenario 1: Jane purchased a Fitbit® six months before she is involved in a car accident. She sues the driver of the other car for neck and back injuries that she claims have caused her to be less active due to constant pain. Jane has worn her Fitbit® ever since she purchased it, including after the accident. Jane could use data from the Fitbit® to show the change in her activity levels post-accident.

Scenario 2: Joe is a criminal defendant charged with armed robbery. Joe's alibi is that he was at home napping when the robbery occurred. However, data from Joe's Apple Watch® indicates that he experienced an abnormally elevated heart rate at the same time of the robbery.

Scenario 3: Jim is suing his former employer for age discrimination which he claims led to his termination. The employer's defense is that Jim was fired because he was a bad employee. In fact, data from Jim's Garmin® watch shows that most afternoons when Jim was supposed to be out of the office meeting with prospective clients, he was actually going for long jogs in the park.

Scenario 4: Jake is bringing a wrongful death lawsuit for the death of his forty year-old wife, who was a school teacher and who wore a Fitbit®. When calculating damages, Jake could hire an expert who could determine her average expected earnings based on her job and also her average life expectancy based on the health patterns recorded by her Fitbit®.

As these scenarios demonstrate, the data collected by activity trackers presents a whole new world of opportunity for supporting, or undermining, claims and defenses in a lawsuit. Yet two very important issues remain: (1) the discoverability, and (2) the admissibility of this information.

Discovering Data from Activity Trackers

In any lawsuit, a frequently contested procedural issue is how much information one party is allowed to "discover" or obtain from the opposing party. For lawsuits in federal court, the rules regarding discoverability are contained in the Federal Rules of Civil Procedure, and courts are often called upon to decide issues related to discoverability and information.

While there is at least one known incident of Fitbit® data being used in a Canadian court in a case similar to the personal injury suit described above in Scenario 1, the use of activity tracker data in U.S. courts still has an uncertain status.

Even though there are no reported opinions in U.S. courts precisely addressing the discoverability of activity tracker information, the Federal Rules of Civil Procedure likely would support the discoverability of this data. Specifically, the Committee Notes from the 2006 Amendments to Rule 34 state that electronically stored information ("ESI") "may exist in dynamic databases and other forms far different from fixed expression on paper" and "electronically stored information stands on equal footing with discovery of paper documents." Thus, Rule 34's definition of ESI is not limited to just emails. Indeed, the Committee Notes specify that ESI should be given a "broad" meaning, and thus it likely includes data from wearable activity trackers. Accordingly, parties would have a duty to produce this data under Rule 34, and a duty to preserve this data or face potential sanctions under Rule 37(e).

Assuming this data is discoverable, from whom should it be requested? There is still uncertainty about who owns the data stored by activity trackers. While this data can be requested from a device wearer, it also can be requested from the provider of the activity tracking service. The terms of use and privacy policies that accompany most activity trackers likely will determine whether it is best to request this data from an opposing party who owns the device or subpoena the information from the third party provider. At least in the criminal context, a recent ruling from the United States Court of Appeals for the Fourth Circuit, which has jurisdiction over federal cases in North Carolina, suggests that activity tracker data can be requested from third party providers without the requirement of a search warrant.

Recently, in United States v. Graham, the Fourth Circuit determined that cell-site location information ("CSLI") could be obtained from a criminal defendant's cell phone provider through a subpoena, without the requirement of a search warrant. The court determined that the defendant's CSLI did not invoke Fourth Amendment search and seizure protections because the information was voluntarily provided to the third party—the cell phone provider. Three of the Fourth Circuit judges, in their partial dissent and concurrence in judgment, noted that the court's decision creates no reasonable "expect[ation of] privacy in data transmitted by networked devices such as the 'Fitbit®' bracelet."
Based on Graham, wearers of activity trackers should expect minimal protections if their data is requested from a third party provider, and activity tracker providers should prepare to receive subpoenas requesting

this information.

The party requesting discovery of activity tracking data should also anticipate that wearers and third party providers will push back. They are likely to claim that the request is overbroad and that there is a lack of proportionality under Rule 26(b)(1), especially since the collected and stored data is often very personal and private in nature. Parties are unlikely to hand over years' worth of their sleep and activity records without putting up a fight. Therefore, requesting parties should be prepared to show the court how this data may lead to information that is relevant to their case. Furthermore, parties requesting this data should consider narrowing the scope of any request so as to avoid a long and tenuous review of years' worth of irrelevant information.

Using Activity Tracker Data in Court

Even if this data can be discovered and analyzed in preparation for litigation, its admissibility into evidence during trial remains unclear because the data reliability is still questionable.

Notably, Fitbit, Inc. ("Fitbit") already has been subject to at least two lawsuits challenging the accuracy of its devices and marketing related to the functionality of its devices. In a 2015 case filed in federal court in Northern California, plaintiffs challenged the accuracy of the Fitbit® sleep tracker function because it tracks movement, not sleep. The claims against Fitbit include unfair competition, false advertising, breach of implied warranty, unfair and deceptive trade practices, common law fraud, and negligent misrepresentation. All of the claims were based on the plaintiffs' allegation that tracking movement is not necessarily a good indicator of sleep quality. Fitbit's motion to dismiss the lawsuit was denied, and the matter is still in litigation.

In January 2016, another lawsuit was filed against Fitbit in federal court in Northern California. This lawsuit included a class of consumer plaintiffs from California, Colorado, and Wisconsin who challenged the accuracy of Fitbit's heartrate monitor. The plaintiffs amended their lawsuit in May 2016 to include allegations based on a university study that compared the Fitbit® heart rate monitor to electrocardiogram ("ECG") heartrate monitoring. The study concluded that the Fitbit® heartrate monitor was inaccurate by an average of about 25 beats per minute when compared to the ECG, and that the Fitbit® often stopped recording wearers' heartrates when they rose above 110 beats per minute.

Thus, the reliability of this type of data may need to be proven, or disproven, at trial through expert testimony. For example, an expert in activity tracker technology could provide testimony explaining the means through which such trackers collect and store data. A judge could then determine if the data is reliable enough to be presented to the jury who would then weigh the credibility of the data based on the expert's analysis. Additionally, an expert could test the accuracy of an activity tracker by, for example, manually counting steps and then comparing that to the number reported by the tracker. Such testing could allow the expert to evaluate the margin of error in a particular tracker's recordings and then testify about the findings.

Tracker device data also may be subject to objections for hearsay, but these objections likely can be overcome through two means. First, if the data is considered hearsay, it may be admissible under the hearsay exception in Federal Rule of Evidence 803(6) for "Records of Regularly Conducted Activity." Second, the data may not necessarily qualify as hearsay under Rule 801 because it may not be offered to "prove the truth of the matter asserted." That is, the data is not offered to prove, for example, that the wearer walked exactly 2,557 steps during a relevant time period, but to prove that the wearer was not asleep or watching a movie as claimed.

Consider Joe from Scenario 2 above. The prosecutor would not be submitting evidence from Joe's Apple Watch® to prove that his heart rate was exactly 170 beats per minute during the time when the robbery occurred—that would be the truth of the matter asserted. The prosecutor just needs to show that Joe's heart rate inexplicably increased during the time of the robbery, which might be unlikely if he were at home napping. If Joe's Apple Watch® on average only tracked 80% of his heart beats per minute, or on average tracked 10% more heart beats per minute than actually occurred, this level of inaccuracy would likely remain constant at all times. Therefore, this consistent, but inexact, measurement would still allow the device to show a significant change in Joe's heart rate, and it could be used to undermine Joe's alibi that he was napping at the time of the robbery.

Conclusion

Much remains unknown about how activity trackers will impact litigation. An increasing number of individuals are purchasing and using these devices each year, and as technology advances, the accuracy of these devices is only likely to improve. With more wearers will come more data collection and, as a result, a greater opportunity for this data to be used in court. Perhaps one day, use of activity tracker data in the courtroom may be as ubiquitous as emails.

--