Get to Know Your Star Witness – Fitbit

Andrew L. Smith, Esq
Smith, Rolfes & Skavdahl Company, L.P.A.

So-called "wearable devices" come in all shapes and sizes with varying features. Ranging from $60 to nearly $200, Fitbit currently offers eight different fitness trackers. Valued at $11 billion, Fitbit is the leader of the wearable device revolution. Similar options include Nike Fuelband and Apple Watch. Companies such as Jawbone, Garmin, Misfit, and Moov Now also offer wearables on the internet and nearly every department store across the country.

Largely known for counting the steps you take, wearables now have all kinds of abilities. According to the Fitbit website, *"Fitbit motivates you to reach your health and fitness goals by tracking your activity, exercise, sleep, weight and more."* "And more" is an understatement. They can track heart rate, workout regimens, skin temperature, sleep habits, and diet. Some can take photographs and video footage, provide call and text notifications, and even search the Internet. Importantly, many wearable devices use GPS to map running routes and track the coordinates of the owner's whereabouts at all times. This information can be accessed in an app and stored on your phone, tablet, or computer.

A wearable device is essentially a pedometer on steroids with GPS. Clearly, wearables are very useful to step up your workout routine. But the information retained on these "mini computers" can also aid in many forms of claims investigations and criminal and civil cases, which we will explore in detail below.

Fitbit Leads to Arrests for Lying to Police and Murder

Police are already using fitness trackers in courtrooms as evidence throughout the country. Law enforcement and legal experts are deeming wearable devices as the human body's very own *"black box."* They can track your every movement 24 hours a day, seven days a week. Wearables provide a "receipt" of human activity, which detectives and police officers now use to evaluate alibis and determine what really happens at crime scenes. Meet your new star eye witness, folks.

The goldmine of evidence kicked off as a result of *Commonwealth v. Risley*, Case No. CP-36-CR-0002937 (C.P. Pa., Lancaster Cnty. Apr. 17, 2015). In Risley, Fitbit established a woman was lying about being sexually assaulted. Ms. Risley traveled to Lancaster, Pennsylvania, where she stayed at her boss' home. The police were called to the home where they found a knife, a bottle of vodka, and furniture in disarray. Ms. Risley notified police she was woken up at midnight and sexually assaulted by a man.

Although she thought she lost her Fitbit during the chaos, the police located Ms. Risley's Fitbit in a hallway. With her consent, the police downloaded data from the device and the Fitbit became the star witness in the alleged rape case. The data showed Ms. Risley was awake, alert, and walking around at the time she claimed she was sleeping. This data, coupled with the boss notifying police Ms. Risley was soon going to lose her position at work, led authorities to discredit the rape allegations. Ms. Risley was then charged with three misdemeanors, including false reports to law enforcement, false alarms to public safety, and tampering with evidence. She pled guilty and had to complete two years of probation for her acts of deceit.

More recently, Fitbit led to a murder arrest in Connecticut. On December 23, 2015, Richard Dabate told the police he took his two children to the bus stop, waved goodbye to his wife, Connie, and went to work. Mrs. Dabate attended an exercise class at the nearby YMCA, with her Fitbit.

Mr. Dabate claimed he then went back home around 9 a.m. because he forgot his laptop. He heard a noise and allegedly went upstairs to investigate. Mr. Dabate allegedly witnessed an intruder at that point. He said he heard Mrs. Dabate return home and yelled for her to run away. Mr. Dabate claims after a short altercation the intruder shot and killed his wife.

The police could not locate any helpful physical evidence at the home. However, the Fitbit provided the following details:

- Movement occurred at 9:23 a.m., the same time the garage door opened into the kitchen.

- While Mrs. Dabate was at home, her Fitbit recorded 1,217 feet of movement between 9:18 a.m. and 10:05 a.m. when all activity stopped.

If Mr. Dabate's statements were true, the police claim the total distance for Mrs. Dabate to walk from her vehicle to the basement, where she was shot, would be a maximum of 125 feet. Mr. Dabate later admitted to having an affair and impregnating the other woman. Just five days after her death, Mr. Dabate also made a claim for her life insurance policy for $475,000.

The combination of the Fitbit data and circumstantial evidence led to Mr. Dabate's arrest on April 14, 2017, for murder, tampering with evidence, and providing a false statement. A trial date has not been set, but you can follow the murder case on the Tolland County Superior Court online docket. *See State v. Dabate,* Case No. TTD -CR17-0110576-T. Mr. Dabate is currently being held at the Hartford Correctional Center on a million-dollar bond.

Wearables in the Civil Context

In 2014, a plaintiff introduced Fitbit evidence in a personal injury case in Canada. The woman used the data to show her physical activity was affected following a car accident.

Likewise, in *Flint v. Strava,* Case No. CGC-12-521659 (Super. Ct., San Francisco Cnty. June 18, 2012), attorneys obtained data from the wearable device company Strava to prove a bicyclist was speeding and at fault for causing his own death after hitting a car. Known as "The Social Network for Athletes," Strava is unique in that the app is designed to connect nearby athletes through the app, and rank them. The plaintiff in *Flint* was attempting to achieve the fastest race pace to regain his first place rank when this accident occurred.

Consider a routine personal injury case where the plaintiff claims his injuries prevent him from engaging in numerous physical activities he engaged in before the accident. He claims to be very active, running 70 miles per week and participating in races and marathons on a regular basis. During the plaintiff's deposition, you learn he wore his Fitbit at all times in the year before the accident. You then request the plaintiff's Fitbit records for the preceding year and discover — contrary to the deposition testimony — the plaintiff would work out two times a week and run a total of eight miles a month.

In employment cases the data can assist in evaluating disability claims, workplace injuries, and even harassment claims. Consider an example where a Nike Fuelband demonstrates the employee's stress level and heart hate increase whenever she is around the alleged harasser at work.

In the insurance defense realm, data obtained from wearable devices can be used in all sorts of ways. Imagine you are investigating a fire loss of a multi-million home located in a rural area. Your origin and cause investigator cannot locate an area of origin due to the size of the home, and he provides a classification of undetermined. The insured, who is self-employed, claims he was driving between job sites at the time of the fire. The insured was waiting for his cell phone to be replaced and he did not have a cell phone that day. However, the insured was wearing a Nike Fuelband his daughter gave him for Christmas.

The GPS tracking data shows the insured had an elevated heart rate the entire hour before the fire. And, most importantly, the GPS data places the insured inside the home just 15 minutes before the home was fully engulfed in flames. I think it is safe to say, the Fuelband just provided a key piece of evidence incapable of being obtained elsewhere.

The following is a list of areas wearable device data can assist us, and this is just the tip of the iceberg:

- Arson Claims
- Theft Claims
- Fraud or Misrepresentation Defense
- General SIU Investigations
- Alibi Verification
- Emotional Distress Allegations
- Personal Injury Cases
- Evaluation of Physical Activities Before and After Accident

How Do We Get It?

So now we know the many types of information wearable devices offer, but how exactly do we obtain this treasure-trove of data? Depending on whether you are at the claims stage or involved in litigation, different options may be available.

CONTINUED

1. You can begin by mining publicly available data and data linked to social media accounts, including Facebook and Twitter. Many individuals will post the results and accomplishments from their workouts on Facebook much the say way as people update their status or check-in to a favorite restaurant. Depending on privacy settings, this may be all you need to do to obtain the data you are seeking.

2. You can request the user's wearable fitness device password and log-in credentials. Next, you can seek the consent of the user, which is exactly what occurred in the criminal investigations discussed above. Whether you obtain the login information or a copy of the stored data from the user's computer, this is a quick and easy option.

3. If you are in litigation, you can use traditional discovery techniques and issue written interrogatories and requests for production of documents to obtain the data.

4. You can also use subpoena power to directly subpoena the data from the wearable device company such as Fitbit or Nike. However, be weary of the procedural "hoops to jump through" using this method. The third-party providers often rely upon the Stored Communications Act and require in-person service of the subpoena before they even consider complying. If you have ever attempted to subpoena other technological companies like Facebook you should expect to confront the same difficulties. If you are not in litigation, you can also consider filing a pre-suit petition for discovery depending upon the state's rules of civil procedure.

Conclusion

Whether you are investigating a minor theft loss or defending a multi-million-dollar personal injury suit, are you using wearable device data to your advantage? As claims professionals and attorneys, devices such as Fitbit offer us a wide array of valuable, easy-to-use, relevant information. Here are a few parting tips regarding the wearable device revolution.

1. Do your research on the different devices on the market and their features. For instance, not every wearable device stores GPS data. Learn how each device works just as if you were researching to purchase a wearable for your own personal use.

2. Consider issuing a discovery preservation letter from the start. The hold letter not only applies to "traditional" ESI, but also to social media postings and wearable device logs and data.

3. When evaluating your discovery options in any claim or case where this data could be relevant, include requests for wearable device data. Also consider the quickest and most efficient mechanism for securing the data.

4. Be prepared to address and respond to evidentiary objections based on the right to privacy, HIPAA, the Federal Food, Drug, and Cosmetic Act, unreliability or inaccuracy of the data, as well as evidentiary rules on hearsay, authentication, relevance, and unfair prejudice.

5. Consider retaining a qualified expert witness to explain and interpret the data you obtain and may rely upon. Likewise, consider addressing discovery of wearable device data with your local electronic discovery management vendor.

Andrew L. Smith is a Partner in the Cincinnati, Ohio office of Smith, Rolfes & Skavdahl Company, L.P.A. who concentrates his practice in the areas of construction law, insurance defense, and bad faith litigation defense. He is the creator of the AGC of Ohio construction law blog, Between the Law and a Hard Hart, and the co-host of BearcatsSportsRadio.com.