CLM
FURTHERING THE HIGHEST STANDARDS OF CLAIMS AND LITIGATION MANAGEMENT
JULY 2017

LEGISLATING UNMANNED AERIAL SYSTEMS

MAJOR DIFFERENCES IN HANDLING MINORS' CLAIMS

THE REAL VALUE OF HIGH-END HANDBAGS

MEET YOUR NEW STAR EYEWITNESS

DATA STORED IN FITBITS AND OTHER WEARABLE DEVICES CAN BE INVALUABLE AT TRIAL AND WHEN EVALUATING CLAIMS

MEET YOUR NEW STAR EYEWITNESS

DATA STORED IN FITBITS AND OTHER WEARABLE DEVICES CAN BE INVALUABLE AT TRIAL AND WHEN EVALUATING CLAIMS

BY ANDREW L. SMITH

Wearable devices come in all shapes and sizes with varying features. Valued at $11 billion, Fitbit is the leader of the wearable device revolution. Fitbit currently offers eight different fitness trackers, ranging in price from $60 to nearly $200.

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. Fitbit devices 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 a phone, tablet, or computer.

A wearable device is essentially a pedometer on steroids and with GPS. Clearly, wearables are very useful for stepping up workout routines. But the information retained by what is essentially a mini computer also can aid in claims investigations and criminal and civil cases.


78

FITBIT ARRESTS

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

Treating a wearable device as a goldmine of evidence kicked off in *Commonwealth v. Risley*. In *Risley*, Fitbit data established that a woman was lying about being sexually assaulted. Jeannine 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. Risley told police that 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 it 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 that Risley was awake, alert, and walking around at the time she claimed she was sleeping. This data, coupled with the boss notifying police that Risley was soon going to lose her position at work, led authorities to discredit the rape allegations. 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 Dec. 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. Connie then attended an exercise class at the nearby YMCA, with her Fitbit.

Richard claimed that he went home around 9 a.m. because he had forgotten his laptop. He said he heard a noise and went upstairs to investigate. Richard allegedly witnessed an intruder at that point. He said he heard Connie return home and yelled for her to run away. Richard claimed that after a short altercation, the intruder shot and killed his wife.

> LAW ENFORCEMENT AND LEGAL EXPERTS VIEW WEARABLE DEVICES AS THE HUMAN BODY'S VERY OWN "BLACK BOX."

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 door between the garage and kitchen opened.
- While Connie was at home, her Fitbit recorded 1,217 feet of movement between 9:18 a.m. and when all activity stopped at 10:05 a.m.

If Richard's statements were true, then the police claimed that the total distance required for Connie to walk from her vehicle to the basement, where she was shot, would be a maximum of 125 feet. Richard later admitted to having an affair and impregnating another woman. Additionally, just five days after his wife's death, Richard made a claim for her life insurance policy valued at $475,000.

The combination of the Fitbit data and circumstantial evidence led to Richard's arrest on April 14, 2017, for murder, tampering with evidence, and providing a false statement. A trial date has not been set, but the murder case can be followed on the Tolland County Superior Court online docket. (See *State v. Dabate*, Case No. TTD -CR17-0110576-T) Richard currently is being held at the Hartford Correctional Center on a $1 million 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*, 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. Referring to itself as "the social network for athletes," Strava is unique in that it is designed to connect nearby athletes through an app and rank them. The deceased in *Flint* was attempting to achieve the fastest race pace to regain his first-place rank when the accident occurred.

Consider a routine personal injury case in which the plaintiff claims his injuries prevent him from engaging in numerous physical activities that he participated 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, the defense learns that he wore his Fitbit at all times of the year before the accident. The defense then requests the plaintiff's Fitbit records for the preceding year and discovers—contrary to the deposition testimony—that 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 of another activity tracker, the Nike Fuelband, which shows the employee's stress level and heart rate increase whenever she is around an alleged harasser at work.

In the insurance defense realm,

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

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

The following is a list of other claims in which wearable device data can be valuable:

- 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 an accident.

HOW DO WE GET IT?

Now that we know the many types of information that wearable devices can provide, how do we obtain this treasure trove of data? Different options are available depending on whether you are at the claims stage or involved in litigation.

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 just as they would update their statuses or check-in to their favorite restaurants. Depending on privacy settings, this may be all you need to do to obtain the data that you are seeking.

WHETHER YOU ARE INVESTIGATING A MINOR THEFT LOSS OR DEFENDING A MULTIMILLION-DOLLAR PERSONAL INJURY SUIT, YOU SHOULD USE WEARABLE DEVICE DATA TO YOUR ADVANTAGE.

Also, you can request the user's wearable fitness device password and log-in credentials, as well as the user's consent, which is exactly what occurred in the criminal investigations discussed earlier. 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.

If you are in litigation, then you can use traditional discovery techniques and issue written interrogatories and requests for production of documents to obtain the data. Additionally, you can use subpoena power to directly obtain the data from wearable device companies such as Fitbit or Nike. However, be aware of procedural difficulties that you may encounter when using this method. The third-party providers often rely on the Stored Communications Act and require in-person service of the subpoena before they consider complying. If you have ever attempted to subpoena other technology companies like Facebook, then you should expect to confront similar difficulties. If you are not in litigation, then you also can consider filing a pre-suit petition for discovery depending on the state's rules of civil procedure.

Whether you are investigating a minor theft loss or defending a multimillion-dollar personal injury suit, you should use wearable device data to your advantage. These devices offer claims professionals and attorneys a wide array of valuable, easy-to-use, and relevant information.

Wrapping up, here are a few parting tips regarding the wearable device revolution.

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

Next, consider issuing a discovery preservation letter from the start. The hold letter not only applies to "traditional" electronically stored information, but also to social media postings and wearable device logs and data.

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

In addition, 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; and evidentiary rules on hearsay, authentication, relevance, and unfair prejudice.

Lastly, 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, LPA. He can be reached at asmith@smithrolfes.com.