2018 Annual Conference
March 14 - 16, 2018
Houston, TX

Alexa, Help Solve My Case!

This panel of attorneys and claims professionals will address the most recent advances in technology and how these gadgets and gizmos can assist us in the world of insurance defense litigation and claims handling. Topics will include: (1) wearable devices such as Fitbit and Nike Fuelband; (2) smart thermostats and smart home systems like Nest; and (3) digital assistants such as Alexa Echo and Dot or Google Home. What information do these devices store? How do we get it? Is it admissible in court? How can we harness this information to our advantage? Alexa is already solving murders across the country. What else can she do for you?

I. Wearable Devices

A. The Options

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.

B. Capabilities

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.

C. Courtroom Evidence

i. Real Life Examples

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.

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.

ii. How We Can Use It

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

iii. Ownership of Data

One issue that may arise is the question of who actually owns the data in the first place, the user or the provider?

For example, the privacy policy of one manufacturer of wearables pledges that they will "let [the user] decide how [their] information is shared." 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."

iv. Evidence Issues

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.

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.

II. Smart Thermostats

A. The Options

Available options include Nest, Ecobee3, Honeywell, Emerson, and Carrier. Nest is by far the most popular device, with $340 million in sales last year alone.

B. Capabilities

Nest stores all the data necessary to provide an energy efficient heating and cooling system. Smart thermostats can link to your digital assistant – the smart home.

C. How We Can Use It

Origin and cause and fire modeling experts can use the data stored on the devices.

Nest includes Home vs. Away Mode. Policy terms, including the Vacancy Exclusion and Abandonment for homeowner's and rental insurance policies are implicated. The data can be useful to investigate claims of theft and robbery.

D. Privacy Issues

The Nest privacy policy includes this language:

> With your consent: We may share personal information when we have your consent."
>
> For legal reasons: We may provide information to a third party if we believe in good faith that we are required to do so for legal reasons. For example, to respond to legal process, or comply with state and federal laws (or the applicable laws of foreign countries other than the United States).

III. Digital Assistants (25 minutes)

A. The Options

The top options include Amazon Echo (and Dot) and Google Home. First introduced in 2014, there are now 8 million Amazon Echo's in use. In 2016 alone

Amazon sold 5.2 million Echo units worldwide. The small version, Amazon Dot, is just $49.99 and will continue to be a popular gift throughout the holidays.

However, the Amazon Echo is not the end –Google Now, Apple's Siri, Windows Cortana, as well as other devices including televisions, game consoles, cars, and toys.

B. Capabilities

The Echo is equipped with seven microphones and responds to a "wake word," most commonly "Alexa." When it detects the wake word, the device lights up blue and begins streaming audio to the cloud, including a fraction of a second of audio before the wake word.

Using Alexa is as simple as asking a question. Just ask to play music, read the news, control your smart home, or tell a joke – Alexa will respond instantly. Whether you are at home or on the go, Alexa is designed to make your life easier by letting you voice control your world.

Alexa lives in the cloud so it is always getting smarter. The more you talk to Alexa, the more it adapts to your speech patterns, vocabulary, and personal preferences. By storing your recordings, Alexa learns more about you than even you know about yourself.

Suffice it to say, Alexa is always listening. The device listens to every word you say. However, according to Amazon, the Echo only begins storing recordings in the cloud *after* the wake word is expressed.

C. Courtroom Evidence

i. Real Life Examples

In November 2015, former Georgia police officer, Victor Collins, was found dead in a backyard hot tub at the Bentonville, Arkansas, home of acquaintance James Andrew Bates. Mr. Bates claimed it was an accidental drowning when he contacted police at 9:30 a.m., claiming he had gone to bed and left Mr. Collins and another man behind in the tub. But Bentonville Police investigators determined Mr. Collins died after a fight, while being strangled and held underwater – and Mr. Bates was the only person at the scene at the time.

Investigators served a search warrant on Amazon in hopes of getting testimony from a possible witness: the Amazon Echo used to stream music near the hot tub when they arrived at the scene. After a flurry of motions and objections by Amazon based on the First Amendment and privacy concerns, Mr. Bates has now consented to disclosure of his Echo data. The case is still pending, and it is not yet known what the Amazon data will demonstrate.

Be sure to follow *State v. Bates*, Case No. 04CR-16-370, Benton County Circuit Court (Feb. 25, 2016), to see what Alexa witnessed the night of Mr. Collins' death.

ii. How We Can Use It

In the insurance defense realm, data obtained from digital assistants 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. The origin and cause expert cannot pinpoint an exact area of origin or a classification of the fire. After Google is subpoenaed, you obtain Google Home data and learn someone was in the house and turned the lights off just 12 minutes before the mansion was engulfed in flames.

Armed with this information, the insurance company's origin and cause expert and your fire modeling expert both agree there is no way the fire could have been accidental. In turn, the insurer denies the claim. The Google Home data could also be relied upon at trial if the insured later sues for breach of contract and bad faith.

In sum, whenever there are potential issues with someone being at the loss location at a particular time, have the digital assistant do what it does best – assist!

- Arson Claims
- Theft Claims
- Fraud or Misrepresentation Defense
- General SIU Investigations

- Alibi Verification

iii. Evidence Issues

So now we know the many types of information digital assistants 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. This analysis is identical to the above discussion with wearable devices.

If you are seeking the data directly from the digital assistant provider, be prepared for a fight. Obtaining data directly from Amazon or Google can be a time-consuming, arduous process. According to Amazon's privacy policy: "Amazon will not release customer information without a valid and binding legal demand properly served on us." Further, "Amazon objects to overbroad or otherwise inappropriate demands as a matter of course."