

Your Employee May Be Wearing His Alibi—Or Your Evidence

(April 2020)

Warren G. Kruse II

Consilio





The following is an article by members of The Sedona Conference's Technology Resource Panel, which was formed in the belief that a well-informed marketplace, speaking in the same language, will ultimately lead to reduced transaction costs for all parties, higher quality, and greater predictability. It represents the opinions of the authors, and your comments and contributions to this discussion are welcome. Click [here](#) for more information on joining the TSC Technology Resource Panel.

Your Employee May Be Wearing His Alibi—Or Your Evidence

By Warren G. Kruse II, Consilio

My Fitbit keeps track of when I'm moving, and when I'm sitting still.

My Apple Watch tells me to stand up.

My Lightscribe pen transcribes my handwritten notes into text on my iPad. It can also record what is being said.

From there, I can send them to my Evernote, which can store everything you can possibly imagine in one workspace, accessible from my phone, tablet, and computer.

My mobile computing device (a.k.a. mobile phone) stores just about anything I need, such as credit cards, receipts, boarding passes, my Starbucks card, my to-do list . . . and I can even make phone calls from it.

It all seems like so much unrelated information—the odds and ends of my daily life, captured by my favorite gadgets. But depending on the devices I use and how I use them, a skilled investigator may be able to define a map of where I've been, what I've been doing, how long I've been doing it, and even who was nearby at the time.

Wearable and mobile technologies are increasingly popular, but most users never think about the data these devices store and use. In the context of an investigation, data from mobile and wearable devices can be an important source of intelligence.

A Rapidly Expanding Market

According to the International Data Corporation's Worldwide Quarterly Wearable Device Tracker, the global wearables market was on track to top 300 million units in 2019 and nearly 500 million units in 2023.¹ Moreover, research and advisory corporation

¹ Worldwide Wearables Market to Top 300 Million Units in 2019 and Nearly 500 Million Units in 2023, Says IDC, BUSINESSWIRE (Dec. 16, 2019, 8:30 a.m.), <https://www.businesswire.com/news/home/20191216005029/en/Worldwide-Wearables-Market-Top-300-Million-Units>.

Gartner, Inc., forecasts that “worldwide shipments of wearable devices will reach 225 million in 2019, an increase of 25.8 percent from 2018. End-user spending on wearable devices is forecast to reach \$42 billion in 2019. Of that, \$16.2 billion will be on smartwatches.”²

Statista, an international provider of market and consumer data, reports: “The wearable market is promising, as the number of connected wearable devices worldwide is expected to jump from 526 million in 2016 to over 1.1 billion in 2022.”³

Wearable Device Data is Already Used in Court

There are now more mobile devices in circulation than there are people in the world, and as the use of these devices and their accompanying applications continues to expand, so too will the body of data sources digital forensic investigators draw upon in their efforts to gather evidence. Moreover, wearable device evidence will also be useful in civil proceedings. Imagine an employee who sues on the basis of a foot injury sustained while on the job—and now imagine defense counsel issuing a discovery request for his Fitbit data, in a bid to show he has been getting around just fine.

John J. Carney of Computer Forensics in St. Paul, Minn., explains how digital devices are transforming litigation: “Exemplary evidence is best evidence. Black’s Law Dictionary defines best evidence as ‘Evidence of the highest quality available, as measured by the nature of the case rather than the thing being offered as evidence. The term is usually applied to writings and recordings.’ Today’s best evidence is often mobile evidence. On a smartphone writings are often text messages, email, and notes. Recordings are often videos, voice messages, and other audio clips.”⁴

Wearable device evidence has already been involved in a variety of court cases, including the following:

- In Gainesville, Fla., a man became a suspect in a burglary when an exercise-tracking app recorded him riding his bicycle past the victim’s home. “Google

² *Gartner Says Worldwide Wearable Device Sales to Grow 26 Percent in 2019*, GARTNER (Nov. 29, 2018), <https://www.gartner.com/en/newsroom/press-releases/2018-11-29-gartner-says-worldwide-wearable-device-sales-to-grow->.

³ *Number of connected wearable devices worldwide from 2016 to 2022*, STATISTA, <https://www.statista.com/statistics/487291/global-connected-wearable-devices/>.

⁴ John J. Carney, *Exemplary Evidence: Mobile device evidence is exemplary evidence*, MINNESOTA LAWYER (Feb. 24, 2020), <https://minnlawyer.com/2020/02/24/exemplary-evidence-mobile-device-evidence-is-exemplary-evidence/>.

tracked his bike ride past a burglarized home. That made him a suspect. Gainesville police, looking for leads, went to an Alachua County judge with the warrant for Google. In it, they demanded records of all devices using Google services that had been near the woman's home when the burglary was thought to have taken place. The first batch of data would not include any identifying information. Police would sift through it for devices that seemed suspicious and ask Google for the names of their users."⁵

- In a sign of the times, the Court of Appeals for the Seventh Circuit became the first circuit court to use the poop emoji in a published opinion.⁶ This was added because many emojis are not searchable, so be careful when doing searches on mobile or social-media data.
- According to police, a Lancaster County woman lied about having been raped by an intruder. The woman claimed to have been sleeping in her home when the attack began, but investigators used data from her Fitbit to show she was walking around during the timeframe in question.⁷
- A law firm in Calgary had the first known personal injury case that used activity data from a Fitbit to help show the effects of an accident on its client.⁸

How do wearables track what you are doing?

Global Positioning System (GPS). Mobile phones use GPS, Wi-Fi and cellular towers to pinpoint your location.

Wi-Fi (wireless computer networking). Every time you turn Wi-Fi on, your phone (or other Wi-Fi enabled device) sends out a signal that includes the device's unique network interface address. Also called the MAC (media access control) address, this is a 12-

⁵ Jon Schuppe, *Google tracked his bike ride past a burglarized home. That made him a suspect*. NBC NEWS (March 7, 2020, 4:22 a.m.), <https://www.nbcnews.com/news/us-news/google-tracked-his-bike-ride-past-burglarized-home-made-him-n1151761>.

⁶ *Emerson v. Dart*, 900 F.3d 469 (7th Cir. 2018).

⁷ Kate Pickles, *Police claim woman lied about being raped after her 'Fitbit' fitness watch showed she had not been dragged from her bed*, DAILY MAIL (June 22, 2015, 10:47), <http://www.dailymail.co.uk/news/article-3134701/Police-claim-woman-lied-raped-Fitbit-fitness-watch-showed-not-dragged-bed.html#ixzz3h0Ju01Rw>.

⁸ Parmy Olson, *Fitbit Data Now Being Used In the Courtroom*, FORBES (Nov. 16, 2014, 4:10 p.m.), <http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/>.

character identifier that is inextricably linked to the device's hardware and can be used to track the device's movements.

Near Field Communication. The set of protocols that enables smartphones and other devices in close proximity to each other to establish radio communication with each other.

Bluetooth. A wireless protocol that connects electronic devices while they are close to each other. Most people will think of their wireless headset, which commonly uses Bluetooth, but Bluetooth is also used to connect wearables to phones, tablets, computers, etc. Standard Bluetooth has a range of about thirty-three feet.

Gyros and Accelerometers. Smartphones and tablets use these sensors to detect the orientation, tilt, and motion of the device. Any change in the orientation of the device (i.e., to look at a picture horizontally, you rotate the device) is measured by the sensor.

Heart Rate Monitor. A variety of different types of heart rate monitors are embedded in wearables. Some, like the Apple Watch and the Fitbit Surge, use an optical heart rate monitor—a sensor that is built into the device itself—but there are also apps that can monitor your heart rate by using your cell phone's camera and flash to capture minute changes in your skin tone that occur with each heartbeat.⁹

Your Employees May be Wearing the Evidence

It is rare to conduct an investigation or an ESI preservation effort that does not involve a mobile device. The increasing popularity of wearable devices further complicates the landscape, from the investigator's perspective, since wearable devices often sync with other devices, both mobile and stationary. SANS Instructor Heather Mahalik, co-author of *Practical Mobile Forensics*, notes that this means investigators in the process of collecting data from a cellphone, tablet, or laptop may also wind up collecting protected information related to an individual's health and fitness.

"The difficulty presented by modern fitness devices is the amount of physical, health, dietary, location and other data the devices collect," noted David Grant, Consilio's deputy general counsel and certified privacy professional. "When companies allow employees to use devices for both work and personal activities, data becomes co-mingled. Companies need to understand the amount of non-company and PII (personally identifiable information) data their employees' devices track and store."

⁹ It should be noted that these are not for medical use and are still being developed.

Yet in spite of these complications, surveys show most organizations either don't have any policy governing use of personally owned devices or have a policy that is unwritten or otherwise inadequate. Moreover, even organizations with a defined policy lack appropriate guidelines regarding how they handle PII that is inadvertently collected, and they generally fail to communicate standards and procedures to their employees.

In order to appropriately address information security, eDiscovery needs, and infrastructure management efforts, organizations must define, implement, communicate, and enforce a so-called BYOD (Bring Your Own Device) policy that addresses all of the various types of personally owned devices that may be permitted in the workplace, including wearables as well as more "traditional" mobile devices. Additionally, policies should cover the following areas:

- **The device itself.** What kinds of devices are specifically allowed in the workplace, and which ones are prohibited?
- **Data.** The policy should address both data stored on or captured by the device, and data the device has access to.
- **Personally Identifiably Information.** How will the organization handle sensitive personal information it may encounter during its efforts to manage discovery of the device?
- **Personally Owned Information.** How will the organization handle personal email, social media posts, and other information that is not related to the individual's professional activities?
- **Privacy laws.** If the organization has employees residing outside the United States, privacy laws governing those employees may be different from those applied to U.S. workers. Policies must take these differences into account and appropriately address employee activities in different jurisdictions.
- **Custody and Control.** According to the Sedona Conference, "an employee may constructively and realistically have both custody and control over a BYOD device. Although the device may hold enterprise 'owned' information; the employee both owns and accesses the data. Without the employee's consent, an employer is not likely to have the ability to both secure control and custody of the device, much less preserve information on the same device."¹⁰

¹⁰ The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 467, 526–27 (2016).

To address this reality, organizations should consider implementing a legal consent form as a part of their BYOD policies. Even if it is a company-owned device, a consent-to-collect waiver can save an organization time and contention, especially if there is a large and growing amount of personal data stored on the device.

- **Termination or Other Exit.** The policy should clearly state what happens to the device and whatever data it holds if the employee leaves the organization voluntarily or is fired.
- **Loss or Theft.** Similarly, the policy should define actions the organization will take to protect any sensitive business information that may have been stored on or captured by the device, if the device is lost or stolen.

Finally, organizations should regularly audit to ascertain whether personally owned devices are in use, and to determine the potential impact on daily operations as well as on the organization's discovery, compliance, and investigative initiatives.

Best Practices for Discovery Management and BYOD

The following habits and practices can help make discovery management involving personally owned devices more thorough and defensible—and less of a headache.

- **Get the password.**

IMPORTANT: If the employee is leaving and turns in a company-owned device, ask them for the PIN/Password/SWIPE needed to access the device. Additionally, ask if encryption was used, and ask whether a backup/sync location was established.

Without this information, if the person leaves and the device is secure, you may not be able to get access to it.

If you are familiar with the device, consider putting the device in **airplane mode** when you assume control of it. This will offer some protection against accidental or intentional wiping of data from the device or accidentally accessing data on other servers that you do not have legal access to.

- **Keep it powered.**

*PRO TIP: INCLUDE
QUESTIONS ABOUT THE
EMPLOYEE'S DEVICE USE IN
YOUR FIRM'S STANDARD
EXIT PROCESS*

Most wearable and mobile devices use solid-state drives—storage devices that use integrated circuits to store data—rather than the disk, motor, and read/write head used in traditional hard drives.¹¹ If your litigation hold involves securing mobile devices “just in case they are needed,” you should be aware that if left unplugged, most solid-state drives are able to retain data for only a limited time. The actual period will depend on various factors including storage temperature. Worst-case scenario, an unplugged solid-state device can retain data for about ninety days; best-case, data may be stored for more than 10 years.¹² With this in mind, when collecting a mobile device, consider collecting its native power connector and keeping the device powered until litigation is completely resolved.

- **Ask good questions.**

Develop a custodian interview form that covers employees’ use of technology, to include personally owned devices and wearables. Key questions include:

- Do you have a company-issued desktop, laptop, cell phone, or tablet? (check all that apply.)
- Do you use any wearable devices? If so, which ones? Do you sync your wearables with other devices, whether company- or personally owned?
- Do you use your company-issued or personally owned device to participate in chats or send texts or group messages for work?
- What apps do you use for work?
- Do you synchronize your phone with a computer or cloud (e.g., iTunes or iCloud)?

About the Author:

Warren G. Kruse II, MSc, CISSP, DFCP, ENCE, is a vice president with [Consilio](#), a provider of eDiscovery, cyber breach review, and data forensic services. He has spent the last twenty-five years between law enforcement and as a consultant supporting various agencies with incident response, computer forensics, and eDiscovery.

¹¹ Solid-state drive, WIKIPEDIA, https://en.wikipedia.org/wiki/Solid-state_drive.

¹² Santosh Kumar & Rajesh Vijayaraghavan, *Solid State Drive (SSD) FAQ*, DELL (October 2011), <http://www.dell.com/downloads/global/products/pvaul/en/Solid-State-Drive-FAQ-us.pdf>.