Your Employee May Be Wearing Their Alibi - Or Your Evidence

Warren Kruse, CISSP, CFCE, EnCE, DFCP
Vice President for Digital Forensics

About the Author

Warren G. Kruse II, CISSP, CFCE, EnCE, DFCP
Vice President, Digital Forensics,
Altep, Inc.
wkruse@altep.com

With more than 30 years' experience in law enforcement and forensic science, Warren is the author of "Computer Forensics: Incident Response Essentials." The diverse range of matters Warren has assisted with includes theft of trade secrets, Wikileaks investigations, misappropriation of intellectual property, breach of contract, internal employment disputes, fraud investigations, and wage and hour class actions, among others. Warren currently serves as the President of the Digital Forensics Certification Board.

Your Employee May Be Wearing Their Alibi - Or Your Evidence

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

My mobile computing device (AKA cell phone) stores just about anything I need, like 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. For example, as is often portrayed on TV, cell phones maintain a call log – and the information in it can be used to determine a user's whereabouts, prove a suspected relationship, and even establish – or disprove – an alibi.

A Rapidly Expanding Market

International Data Corporation, a noted technology research group, has recently reported that the total volume of smart "wearables" will reach 25.7 million units in 2015, boosted by the Apple Watch. "Smart wearables are about to take a major step forward with the launch of the Apple Watch this year," said Ramon Llamas, Research Manager with IDC[1].

Moreover, the market for wearable technology is set to grow from $1.6 billion to $5 billion, according to research by Gartner[2].

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.

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

- 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[3].
- A law firm in Calgary is working on the first known personal injury case that will use activity data from a Fitbit to help show the effects of an accident on their client[4].
- 26-year-old Derek Kellett faces five counts of reckless driving after he shot a series of videos while wearing a GoPro. In the videos, which Kellett subsequently posted on YouTube, he drives at speeds up to 115 mph[5].

How Do Wearables Track What You Are Doing?

Global Positioning System (GPS). Mobile phones use GPS, WiFi 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 address, this is a 12-character identifier that is inextricably linked to the device's hardware, and can be used to track the device's movements.

Near Field Communication (NFC). 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 another. 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. you want to look at a picture horizontally so you turn 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 which 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 heart beat[6].

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 only 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.

David Grant is Altep's Director of Privacy Services. "The difficulty presented by modern fitness devices is the amount of physical, health, dietary, location and other data the devices collect," Grant noted. "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 data and personally identifiable information their employees' devices track and store."

In spite of these complications, however, surveys show most organizations either don't have any policy governing use of personally-owned devices, or have a policy which 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 generally fail to communicate standards and procedures to their employees.

In order to appropriately address information security, e-discovery 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 both wearables and 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 company handle sensitive personal information it may encounter during its efforts to manage discovery of the device?

Personally Owned Information. How will the company handle personal email, social media posts, and other information that is not related to the individual's professional activities?

Privacy laws. If the company has employees residing outside the U.S., 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 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."

To address this reality, companies 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 you time and help avoid disputes, 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 company voluntarily or is fired.

Loss or Theft. Similarly, the policy should define actions the company 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, companies 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 company's discovery, compliance, and investigative initiatives.

Best Practices for Discovery Management and BYOD

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

Get the Password

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.

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

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

Keep it Powered

Most wearable and mobile devices use solid state drives – storage devices which use integrated circuits to store data, rather than the disk, motor, and read/write head used in traditional hard drives[7]. 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 only able to retain data for a limited time. The actual period will depend on various factors, including storage temperature. Worst case, an unplugged solid state device can retain data for about ninety days; best case, data may be stored for more than 10 years[8]. 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 which 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)?

For more information on BYOD

Download additional resources and whitepapers from http://forensics.altep.com:

- Mobile Devices in Electronic Discovery
- Auditing for Personally-Owned Devices
- Forensic Acquisition and External Storage

For further reading:

Data From Our Wearables Is Now Courtroom Fodder:

---

[1] http://www.forbes.com/sites/theopriestley/2015/06/27/goodbye-apple-watch-hello-again-g-shock/

[2] http://www.computerweekly.com/news/2240223173/Wearable-technology-new-privacy-headaches-for-employers

[3] http://www.dailymail.co.uk/news/article-3134701/Police-claim-woman-lied-raped-Fitbit-fitness-watch-showed-not-dragged-bed.html#ixzz3h0Ju01Rw

[4] http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/

[5] http://www.foxcarolina.com/story/25645528/police-man-fled-from-officers-posted-gopro-video-on-youtube#ixzz3h0lPyRuj

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

[7] https://en.wikipedia.org/wiki/Solid-state_drive

[8] http://www.dell.com/downloads/global/products/pvaul/en/Solid-State-Drive-FAQ-us.pdf

WITH **OFFICES** THROUGHOUT **THE UNITED STATES** AND IN **EUROPE,**

NO MATTER WHERE YOU ARE, **WE'LL BE THERE**

CONSULTING

Litigation Readiness
30(b)(6) Witness
Subject Matter Experts
e-Discovery Liaisons
Data Incident Investigations
Data Privacy Experts
Compliance Risk Assessment

DIGITAL FORENSICS

High Tech Investigations
BYOD Strategy
Expert Testimony
Standard & Non-Standard Data Acquisition
Incident Response

DISCOVERY

Collection
Early Data Assessment
Electronic Data Discovery
Paper Discovery
Secure Hosting and Review
ESI Vault®

www.altep.com • 800.263.0940

20150506