**Exemplary Evidence**

**Working Title: Fitness Trackers are Killing Our Opportunity to Lie**

**Caption/Teaser: Wearable devices like Fitbits and Apple Watches are becoming materially important sources of evidence upon which criminal and civil cases may turn in court. Whether the activity, health, or location evidence is found in the fitness tracker, the smartphone paired to it, or the connected, online cloud account, its recovery has the power to deliver the facts, difficult to dispute, that speak to the truth.**

**Author: John J. Carney, Esq., Chief Technology Officer**
**Carney Forensics, www.carneyforensics.com**

Depending upon which information technology research company you follow, each of us in the U.S. this year uses between three to four smart devices connected to the Internet. Often the user profile looks something like this – a smartphone, a tablet, a wearable fitness tracker, and a smart speaker. [Smart speakers are next month's Exemplary Evidence.] Each smart device is equipped to record voluminous amounts of personal, even intimate, information about our digital lives. We lawyers refer to it in a jurisprudence context as electronically stored information (ESI). It is discoverable in both criminal and civil matters in federal and state courts and is increasingly the responsive evidence used to decide or settle cases.

ESI from fitness trackers, digital watches, or other wearable devices is having an impact. During the past five years we have seen it emerge in cases of first impression in personal injury and wrongful death. In criminal matters we're seeing it primarily in homicides, but also criminal sexual conduct cases. "Ninety-nine percent of crime will now have a digital component," says Jonathan Rajewski, a digital forensics instructor at Champlain College in Vermont. "We have these little sensors all over. We're wearing them and they're in our homes." Nicole Chauriye, a J.D. Candidate in 2016 at the Columbus School of Law (Catholic University of America) put it even more succinctly in her law review article, "Technology is Killing Our Opportunity to Lie". Nicole Chauriye, Wearable Devices as Admissible Evidence: Technology is Killing Our Opportunity to Lie, 24 Cath. U. J. L. & Tech (2016).

***Fitbit Trackers***

Fitbit sold about 16 million units of its smart fitness trackers last year bringing its user base to over 27 million persons. Fitbit's activity types include walking, running, swimming, and sleeping. Activities are measured in steps walked, floors climbed, heart rate, and sleep activity and quality. Activity metadata (the data about the data) includes date and time stamps, distance, duration, speed, and pace. Fitbit's location types include position and journeys with date and time stamps from exercise activities. Courts are noting fitness tracker devices which "collect data about a user's steps walked, calories burned, activity intensity, sleep, and other health and fitness metrics . . . devices also connect to the internet . . . allow[ing] the user to view and analyze the data collected. . ." *Fitbug Ltd. v. Fitbug, Inc.*, 78 F.Supp.3d 1180 (N.D. Ca. 2015).

Fitbit records were first used as evidence in a murder trial in Ellington, Connecticut. Connie Dabate was shot to death in December 2015 during what her husband Richard said was a violent home invasion. But Police say it was actually Richard who pulled the trigger, killing his wife after getting his girlfriend pregnant. Connie's Fitbit contradicted Richard's story, as it showed his wife was moving around her house nearly an hour after the time he said she was shot dead. The Fitbit's data showed she had walked 1,217 feet after returning home, far more than the 125 feet it would take her to go from the car in the garage to the basement in Richard's telling of what happened. Five days after Connie was killed, Richard Dabate tried to claim his wife's $475,000 life insurance policy, but was rebuked by the insurance company. Connie's sister filed a wrongful death suit against him.

Keith Diaz, an assistant professor of behavioral medicine at Columbia University Medical Center, testified as an expert witness at the trial. He studied the accuracy of Fitbits and similar devices in measuring physical activity and testified that a variety of scientific studies have found that Fitbits, especially the kind found on Connie Dabate's body when she was killed, accurately report physical activity. "It's particularly useful and accurate for step counts," Diaz said. Under cross examination, Diaz acknowledged the error rate is about 10% for Fitbit use by people in real world conditions rather than in a lab. "The devices tend to overestimate step counts", he said, "but they are still viewed as reliable measuring devices."

In another Fitbit criminal case Lancaster County Pennsylvania law enforcement said a woman lied about an unknown man raping her at knifepoint. She claimed to have been sleeping when the sexual assault began, but investigators probed evidence from her Fitbit fitness tracker and found she had been walking when she said she was sleeping. Police allege the Fitbit, combined with other circumstances, showed the scene was staged and the woman knowingly filed a false report.

The first known personal injury case producing activity evidence from a Fitbit was litigated in Calgary, Alberta in 2014 to show the effects of a motor vehicle accident on the plaintiff's exercise and activity levels. Attorneys for the woman introduced the evidence to show her level of activity post-accident was below the norm for someone of her age and engaged in her profession of personal training. Fitness tracker evidence can also go the other way according to legal blogger Neda Shakoori quoted in Forbes, "The data generated by the plaintiff's wearable device may be discovered in litigation and, as a result, completely discredit plaintiff's case for damages resulting from the accident."

***Apple Health on Apple Watches and iPhones***

Apple's Health app, pre-installed on all iPhones, has provided crucial evidence in Germany in which the suspect was charged with rape and murder. A nineteen-year-old medical student was strangled and drowned in a river in October 2016. The suspect's iPhone geolocated his movements in the crime scene area and the Apple Health app identified periods of strenuous activity, including two peaks. The app recorded the suspect's activity as climbing stairs which supports the investigator's theory he dragged his victim down a riverbank and climbed back up. The local Chief of Police told the court, "For the first time, we correlated health and geo-data."

***Recovery of Fitness Tracker Evidence***

So how is fitness tracker evidence recovered forensically? Three methods come to mind based on where the evidence resides. It can be recovered from the fitness tracker itself. Whether it's an Apple Watch, a Garmin Watch, or one of many Android watches running Google's Wear OS, there are ways to collect the evidence forensically. But that's not the first place I would look.

The smartphone paired to the fitness tracker using Bluetooth or near-field communication (NFC) is a good bet because the digital evidence is likely to be synched to the phone. Mobile device forensic tools to recover smartphone evidence are mature technology featuring highly probative extractions and support for hundreds of mobile apps including those used by fitness trackers. And many more examiners are trained in mobile device forensics and certified on their usage.

But the third method of forensically recovering fitness tracker evidence is often the best. The online cloud account subscribed to by the fitness tracker user is accessible and often the hub for its data. Apple Watches and iPhones synch their activity data to the user's iCloud account. Fitbits do the same to the user's Fitbit cloud account. Garmin Watches synch activity and location data to their user's Garmin Connect account. And we could go on about Google Fit and Samsung Health accounts. Examiners probe and collect these accounts with legal authority using cloud forensic tools with good success every day. But these accounts also support data exports and user downloads for subscribers themselves to get their hands and minds on their own activity and health evidence.

*Next month Exemplary Evidence will explore the digital forensics of smart speakers, including Amazon Alexa and Google Home (Nest) for the discoverable evidence these popular devices collect and the privacy issues that ensue.*