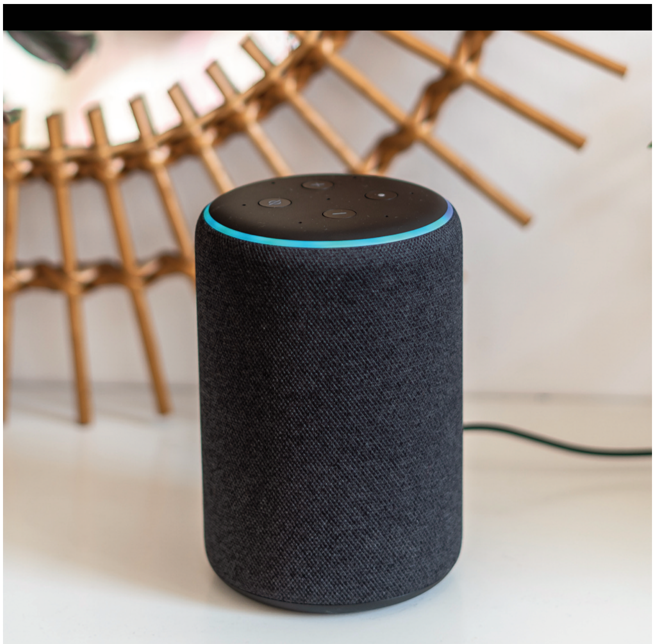

Alexa, Testify

New sources of evidence from the internet of things.

BY JOHN G. BROWNING AND LISA ANGELO

Few areas illustrate the changing nature of the practice of law more than the explosion of sources of digital evidence that can play a game-changing role in civil and criminal cases. In our increasingly wired, data-driven world, the number of web-enabled devices that make up the "internet of things" is projected to nearly triple from 13.4 billion in 2015 to 38.5 billion in 2020.[1] Consumers are filling their homes with everything from "smart" kettles and refrigerators to interconnected lightbulbs, doorbells, toothbrushes, baby monitors, and medical devices. Wearable technology, including activity/fitness trackers like the Fitbit or Apple Watch, has also helped usher in the "IoT" revolution, providing a digital treasure trove of insight into the health and lifestyle of the device's wearer for enterprising attorneys. But along with the incredible growth of the internet of things and the unprecedented information-gathering by these devices come dramatic new concerns about consumer privacy, data security, and the potential uses for such data in the civil and criminal arenas.

There's no shortage of examples to illustrate this changing evidentiary landscape. For example, in February 2017 police in Middletown, Ohio, charged 59-year-old Ross Compton with aggravated arson and insurance fraud after data from his pacemaker was inconsistent with his account of his physical activity when his home burned down. Compton claimed he had frantically packed some belongings, broken the glass of a bedroom window to get out, and scrambled to escape. But with their suspicions raised by the telltale smell of gasoline at the scene and on Compton's clothing, police got a search warrant to look at data from the man's pacemaker. A cardiologist reviewed the heart monitor's data and concluded that Compton's story was "highly improbable."[2]

In the 2015 Pennsylvania case of *Commonwealth v. Risley*, Jeannine Risley claimed that an intruder had sexually assaulted her at a home owned by her employer. She alleged that she had been sleeping at the time, but police were suspicious, especially when she contradicted herself about the whereabouts of the Fitbit she had been wearing. After locating the Fitbit and retrieving and analyzing its data, they learned Risley had been awake, actively walking around—not sleeping—before and at the time of the alleged assault. She was later charged with filing a false report.[3]

In December 2015, Richard Dabate, of Ellington, Connecticut, told police an intruder had broken into his home, killed his wife, Connie, and then beaten him before tying him to a chair. With no witnesses and no suspects, police began searching for digital clues, searching everything from the house's smart home security system to Connie Dabate's Fitbit. The fitness tracker contradicted Richard's story in multiple ways, refuting the time of her murder and demonstrating that Connie had walked 1,217 feet after getting home (rather than being killed immediately upon her return, as Richard had claimed). Through subsequent questioning of Richard, police learned he had a pregnant girlfriend whom he had promised to marry after divorcing Connie. The husband remains free on $1 million bail while awaiting trial.[4]

Of course Fitbit data can be used not just to contradict the guilty, but also to vindicate the innocent. In 2018, after the brutal murder of Nicole VanderHeyden, a young mother of three in Green Bay, Wisconsin, who was beaten to death and left in an open field, defense attorneys for the chief suspect George Burch tried to divert blame onto VanderHeyden's boyfriend, Douglass Detrie. But Detrie was wearing a Fitbit when the murder occurred, and prosecutors' examination of the fitness tracker showed that Detrie's minimal movements at the time of the crime were completely inconsistent with the savage beating of the victim and then dragging her body to a field.[5] And given the wealth of data that such fitness trackers collect and store—steps taken, duration, intensity level, distance traveled, calories burned, sleep quality, etc.—they can also provide highly useful information in civil cases. In a late 2014 personal injury case in Canada, the plaintiff's attorney for an injured personal trainer used his client's Fitbit data to support her claims about the accident's effect on her post-injury activity level. The attorney used an analytics company, Vivametrica, to study and compare the plaintiff's information with the general population and to illustrate how the injuries had affected her condition.[6]

Fitness trackers aren't the only source of valuable digital evidence; Alexa is, too. Alexa is the virtual assistant of Amazon's Echo, a web-connected wireless speaker that, upon voice command, can provide music and information on a variety of topics. Always listening through multiple built-in microphones, the Echo also records up to 60 seconds of sound from its surroundings (streaming this audio into the cloud), including a fraction of a second before its "wake word." Prosecutors in the case of *State of Arkansas v. James Andrew Bates* sought such Amazon Echo data to explain the November 22, 2015, death of Victor Collins, found dead in the hot tub of James Bates' Bentonville, Arkansas, home. Bates claimed he had been asleep and awoke to find Collins face down in the water. Police maintained there was evidence of a struggle, and prosecutors hoped to see if Bates' Amazon Echo had recorded anything, so they subpoenaed Amazon's records. Amazon initially resisted the prosecution's request but later provided the data when Bates agreed to voluntarily turn over the recordings. Ultimately, in December 2017, the prosecutors voluntarily dismissed the murder charge, with Bates insisting all along that Collins' death had been a tragic accident.[7]

And was Alexa listening when Christine Sullivan was stabbed to death in her Farmington, New Hampshire, home on January 27, 2017? Prosecutors believe an Echo device in the house may have captured evidence establishing the guilt of Sullivan's live-in boyfriend, Timothy Verrill, in the murder of Sullivan and her friend, Jenna Pellegrini. They contend that Verrill, with ties to various criminal activities, murdered the two women over suspicions that they were informing police about an alleged drug ring implicating him. The court found probable cause to believe the Amazon Echo device contained recordings that constituted evidence of the crimes, and ordered Amazon to turn over the data. Amazon has initially refused, stating it will "not release customer information without a valid and binding legal demand properly served on us."[8] Amazon says that it receives fewer than 500 search warrants annually for Echo stored data (complying with fewer than half of the orders). But with recent estimates indicating that about 16% of American homes have some sort of smart speaker listening in on their lives, it would not be surprising for that figure to rise.

The impact of these new sources of digital evidence is hardly an American phenomenon. In 2018, data from Apple's Health app proved pivotal in prosecuting a man for the October 2016 murder of medical student Maria Ladenburger in Freiburg, Germany. The data from the app on the defendant's iPhone not only pinpointed his movements, but also suggested periods of more strenuous activity that matched police investigators' recreation of how the defendant disposed of the body. Faced with such digital evidence, the defendant admitted his guilt.[9] In January 2019, Liverpool, England, hitman Mark "Iceman" Fellows was found guilty of the murders of two rival gangsters—thanks to evidence from his Garmin GPS watch. Police had trouble linking Fellows to the crimes, until they noticed a photo of Fellows—an avid runner and cyclist—competing in a local 10K race and wearing a Garmin Forerunner device. Detectives found the watch in Fellows' home, searched its GPS data for information, and found data placing him at both murder scenes at the times of each murder. Fellows was sentenced to life in prison.[10]

In Australia, prosecutors used data from 57-year-old Myrna Nilsson's Apple Watch to help solve her September 2016 murder. Nilsson's daughter-in-law, Caroline Nilsson, claimed that the woman was killed in a home invasion by a group of intruders who had tied her up. Forensic analysis of the data on the watch revealed a seven-minute window between the attack and Myrna's death, which contradicted Caroline's account of the attack and its timeframe. While she had been a prime suspect, Caroline Nilsson was only charged with her mother-in-law's murder after the Apple Watch data came to light.[11]

Civil litigators, prosecutors, and criminal defense attorneys all need to be aware of the gold mine of information that may be sitting on a client's wrist or in their living room. And while there are obvious benefits, there are concerns as well, ranging from evidence preservation issues to data retrieval and admissibility issues. Additionally, in the wake of consumer class actions involving fitness trackers like Fitbit, questions about the reliability of such data will no doubt be raised along with concerns over data privacy and constitutional challenges based on Fourth Amendment protections. In addressing these concerns, courts will be in the unenviable position of applying laws that never envisioned such technology—and judges won't be able to ask Alexa for help. **TBJ**

Notes

[1] John G. Browning, "*Alexa, Will You Testify Against Me?*" Dallas Bar Headnotes (April 2017), http://www.dallasbar.org/book-page/alexa-will-you-testify-against-me; *see* https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020.

[2] Marguerite Reardon, *Your Alexa and Fitbit can testify against you in court*, CNET (Apr. 5, 2018), https://www.cnet.com/news/alexa-fitbit-apple-watch-pacemaker-can-testify-against-you-in-court/.

[3] Katherine Vinez, *The Admissibility of Data Collected From Wearable Devices*, 4 Stetson J. Advoc. & L. 1 (2017), https://www2.stetson.edu/advocacy-journal/the-admissibility-of-data-collected-from-wearable-devices/.

[4] *Supra* note 2.

[5] Tom Messina, *How a Fitness Tracker Can Solve Crimes*, Above The Law (Oct. 16, 2018), https://abovethelaw.com/2018/10/how-a-fitness-tracker-can-solve-crimes.

[6] *Supra* note 3.

[7] Nicole Chavez, *Arkansas judge drops murder charge in Amazon Echo case*, CNN (Dec. 2, 2017), https://www.cnn.com/2017/11/30/us/amazon-echo-arkansas-murder-case-dismissed/index.html.

[8] Meagan Flynn, *Police think Alexa may have witnessed a New Hampshire double homicide. Now they want Amazon to turn her over*, The Washington Post (Nov. 14, 2018), https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over/.

[9] *Apple health data used in murder trial*, BBC (Jan. 12, 2018), https://www.bbc.com/news/technology-42663297.

[10] Emily Caron, *Hitman Runner Convicted of Mob Boss Murders on GPS Watch Tracking Data*, www.si.com (Jan. 17, 2019), https://www.si.com/track-and-field/2019/01/17/british-hitman-runner-mark-fellows-convicted-mob-murders-gps-watch-tracking.

[11] Rhett Jones, *Apple Watch Health Data Is Being Used as Evidence in an Australian Murder Trial*, Gizmodo (Apr. 3, 2018), https://gizmodo.com/apple-watch-health-data-is-being-used-as-evidence-in-an-1824265652.

JOHN G. BROWNING

is a partner in Passman & Jones in Dallas, where he handles commercial litigation, employment, health care, and personal injury defense matters in state and federal courts. He is an award-winning legal journalist for his syndicated column, "Legally Speaking," and is the author of the Social Media and Litigation Practice Guide *and a forthcoming casebook on social media and the law. Browning is an adjunct professor at SMU Dedman School of Law.*

LISA ANGELO

advises clients on data privacy, cyber insurance disputes, breach response, technology transactions, and other matters related to technology and cyber law. She has two internationally recognized certifications in information privacy: a Certified Information Privacy Manager and Certified Information Privacy Professional/US. She is licensed to practice law in Texas and Colorado.