Richmond Journal of Law & Technology

Volume 22 | Issue 3 Article 4

2016

# A Litigator's Guide to the Internet of Things

Antigone Peyton

# A LITIGATOR'S GUIDE TO THE INTERNET OF THINGS

Antigone Peyton, Esq.*

Cite as: Antigone Peyton, *A Litigator's Guide to the Internet of Things*, 22 RICH. J.L. & TECH. 9 (2016), http://jolt.richmond.edu/v22i3/article9.pdf.

## I. INTRODUCTION

[1] Maybe you've heard about the Internet of Things (IoT). It's the network of physical objects (or "things") that connect to the Internet and each other and have the ability to collect and exchange data. It includes a variety of devices with sensors, vehicles, buildings, and other items that contain electronics, software, and sensors. Some IoT objects have "embedded intelligence," which allows them to detect and react to changes in their physical state.[1] Though there is no specific definition of IoT, the concept focuses on how computers, sensors, and objects interact with each other and collect information relating to their surroundings.[2]

* Antigone Peyton is the founder and CEO of Cloudigy Law PLLC, an intellectual property and technology law firm located in McLean, Virginia. Antigone is an unabashed technophile focused on intellectual property litigation and cutting-edge legal and emerging technology issues, particularly those involving social media, patents, trademarks, copyrights, and trade secrets. Antigone is a frequent speaker and writer covering technological competence, IP, social media, and e-Discovery issues. You can find her on Twitter (@antigonepeyton) or on SnapChat (assuming you know what it is and how to use it).

[1] *See Embedded Intelligence – Connecting Billions of Smart Sensors Into the Internet of Things*, ARM HOLDINGS, http://ir.arm.com/phoenix.zhtml?c=197211&p=irol-embeddedintelligence, *archived at* https://perma.cc/3HWX-QBWW (last visited Mar. 23, 2016).

[2] The "things" or "objects" in the IoT generally do not include desktop or laptop computers, smartphones, and tablets.

[2] In 2009, the number of "things" connected to the Internet surpassed the number of people worldwide.[3] That was just the beginning of the IoT movement.[4] In fact, some industry experts estimate that there will be up to 50 billion connected devices by 2020.[5] The LinkedIn "Internet of Things Community" is 12,000 members strong, and it's growing every day.[6] Lawyers need to understand how this explosive growth in the IoT market is going to change their practice in the courtroom.

[3] From a litigator's perspective, there are benefits and risks associated with IoT evidence. These connected objects, combined with big data analytics, can make cases simultaneously clearer and more complicated. The IoT movement also challenges litigators to roll up their sleeves and think creatively about how all these connected objects can tell a story. The key evidence that blows the case wide open may be right in

---

[3] *See* DAVE EVANS, CISCO INTERNET BUS. SOLUTIONS GRP., THE INTERNET OF THINGS: HOW THE NEXT EVOLUTION OF THE INTERNET IS CHANGING EVERYTHING 3 (2011), http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf, *archived at* https://perma.cc/HDF9-NM6T.

[4] *See* ACCENTURE, THE INTERNET OF THINGS: THE FUTURE OF CONSUMER ADOPTION (2014), https://www.accenture.com/t20150624T211456__w__/us-en/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Global/PDF/Technology_9/Accenture-Internet-Things.pdf, *archived at* https://perma.cc/JKG7-UT4P.

[5] *See* EVANS, *supra* note 3, at 3. IDC's Digital Universe study reports that by 2020, there will be 200 to 300 billion connected IoT objects. *See The Digital Universe of Opportunities: Rich Data and the Increasing Value of the Internet of Things*, EMC$^2$ (Apr. 2014), http://www.emc.com/leadership/digital-universe/2014iview/internet-of-things.htm, *archived at* https://perma.cc/86RJ-786G; *see also Data Set to Grow 10-fold By 2020 As Internet of Things Takes Off*, COMPUTERWEEKLY.COM (Apr. 9, 2014, 1:00 PM), http://www.computerweekly.com/news/2240217788/Data-set-to-grow-10-fold-by-2020-as-internet-of-things-takes-off, *archived at* https://perma.cc/KGW9-K7DF.

[6] *See Internet of Things Community*, LINKEDIN, https://www.linkedin.com/groups/4662022/profile, *archived at* https://perma.cc/2CPN-EAXX (last visited Mar. 23, 2016).

front of your face, flying through the interweb, waiting patiently in a client's smart phone app, or sitting on their fitness device.

[4] For instance, and as this paper explores, IoT information can be used to track suspects' movements at the time a crime occurred and provide evidence of an alibi. It can be used to attack the credibility of witness testimony and show how a vehicle was (or wasn't) functioning properly when an accident occurred. As with all evidence we might use in the courtroom, lawyers, juries, and judges need to understand how IoT data should be interpreted and its limitations.

[5] Lawyers also need to talk with clients about the smart objects they interact with and which objects might have information that is potentially relevant to litigation. The data those objects collect might reflect a client's physical injury and diminished capacity, indicate the physiological response to a sexual harassment incident, or provide evidence of a former employee's unauthorized access to company systems to steal data. Consider the narrative that can be created once you obtain the right IoT data from a client or opponent. You can't consider the options, however, until you ask the right questions.

[6] It's time to hone your technical competence and start thinking about how IoT will forever change the way you prepare and try your case! This is the litigator's guide to the Internet of Things.

## II. THE INTERNET OF WHAT?

[7] The basic premise behind IoT is that everyday objects can be turned into "smart" devices that operate better, are more efficient, and communicate with their people masters and other objects. These objects are programmed to communicate via apps, text messages, browsers, and other tools. They tend to communicate using embedded sensors and wired

and wireless communication protocols and systems, including Wi-Fi, Bluetooth, and a variety of specialized IoT protocols.[7]

[8] Imagine a refrigerator that tells you when you need more milk,[8] or a home thermostat that can be adjusted remotely using an app on your mobile device and learns your behavior patterns relating to your home climate.[9] Or a networked house that connects power outlets to sounds systems, TVs, smoke detectors, security cameras, coffee pots, and the home owner through a software app.[10] These homes already exist,[11] and more are coming online everyday.

---

[7] Current IoT products are communicating through a variety of communication platforms and standards, including new home automation standards produced by Google (Brillo/Weave) and Apple (HomeKit) that connect each company's devices in a proprietary communication network.

[8] *See* Michael Gowan, *LG Smart Fridge Spots Spoiled Food, Orders Groceries*, NBCNEWS.COM, http://www.nbcnews.com/id/50364798/ns/technology_and_science-tech_and_gadgets/t/lg-smart-fridge-spots-spoiled-food-orders-groceries/#.VvNWzmQrL6c, *archived at* https://perma.cc/6JXM-ZUY7 (last updated Jan. 4, 2013, 12:46 PM) (explaining how LG's smart refrigerator connects to the Internet, allowing users to remotely access the refrigerator content list, keep track of their grocery list, and identify out-of-date products stored in it).

[9] *See* Bernard Marr, *Google's Nest: Big Data And The Internet of Things In The Connected Home*, FORBES (Aug. 5, 2015, 10:52 AM), http://www.forbes.com/sites/bernardmarr/2015/08/05/googles-nest-big-data-and-the-internet-of-things-in-the-connected-home/#5a41706b58a1, *archived at* https://perma.cc/F2SQ-F867 (discussing the Nest thermostat and the usage data uploaded from individual devices via the Internet, which allows Nest to understand energy usage trends across community microcosms and around the world).

[10] *See, e.g.*, *A Smart Home Solution That Lives in the Cloud*, COMCAST, http://corporate.comcast.com/news-information/news-feed/the-future-of-the-home-bringing-the-power-of-the-cloud-to-home-management, *archived at* https://perma.cc/CR59-UF3J (last visited Mar. 23, 2016) (describing the Xfinity Home technology, which allows users to monitor and control security cameras, smoke detectors, thermostats, lights, and motion sensors through web browsers or Internet connected devices); *see also* Marr, *supra* note 9 (discussing how Google is building infrastructure for smart homes of the future that are fully networked by its own devices).

[9] This increased connectivity includes objects outside the home. Workers and service professionals are connecting remotely and communicating with their company's business equipment and office systems via mobile devices.[12] Consumers are buying networked cars,[13] and walking around with wearable fitness and health technologies strapped to their arms and embedded in their clothes that track their vitals and activity levels.[14] Bikers are using apps and devices to track their workouts and film their surroundings.[15] Google Glass wearers are creating and recording information as they travel and they are communicating with the Internet using voice commands.[16] All of these connected technologies create interesting information about their users and have some level of situational awareness.

---

[11] *See* Daniel H. Wilson, *Smart House: Your So-Called Sci-Fi Life*, POPULAR MECHANICS (Sept. 30, 2009), http://www.popularmechanics.com/technology/gadgets/a4109/4216434/, *archived at* https://perma.cc/R3LT-HH69.

[12] *See* Angela Moscaritolo, *Your Printer Can Now Order Ink for You, Thanks to Amazon,* PCMAG.COM (Jan. 19, 2016, 11:35 AM), http://www.pcmag.com/article2/0,2817,2498102,00.asp, *archived at* https://perma.cc/9HRR-R6MT.

[13] *See* Brendan O'Brien, *The Cloud-Connected Car Drives IoT Monetization,* TECHCRUNCH (Oct. 20, 2015), http://techcrunch.com/2015/10/20/the-cloud-connected-car-drives-iot-monetization/, *archived at* https://perma.cc/7NJJ-VV8K.

[14] *See* James Stables, *Best Fitness Trackers 2016: Jawbone, Misfit, Fitbit, Garmin and More*, WAREABLE (Mar. 7, 2016), http://www.wareable.com/fitness-trackers/the-best-fitness-tracker, *archived at* https://perma.cc/HF2M-BJU9.

[15] *See* Elisha Hartwig, *5 Apps to Map Your Bike Route*, MASHABLE (Sept. 11, 2013), http://mashable.com/2013/09/11/bike-route-apps/#nIAaDJ1kfEqZ, *archived at* https://perma.cc/E8D9-HTHM.

[16] *See* Matt Swider, *Google Glass Review,* TECHRADAR (Feb. 20, 2015), http://www.techradar.com/us/reviews/gadgets/google-glass-1152283/review, *archived at* https://perma.cc/6NW4-FLK3.

## III. THE CONNECTED STATE

### A. Connected Toys

[10] There are a surprising number of everyday objects found in homes that are recording information and transmitting it offsite. One creepy example of the IoT revolution is Mattel's talking Barbie.[17] Mattel's connected Barbie can talk with your child through an embedded microphone and a Wi-Fi connection that's engaged when you hold down a button on her belt.[18] When someone talks to "Hello Barbie," the conversation is recorded and sent to a server back at the company that makes the voice recognition technology powering Barbie.[19] There, speech recognition software (think of a Barbie version of Siri) interprets the child's statements and sends back a pre-programmed response.[20] That's right, the doll talks back to the child. Mattel's partner, ToyTalk, stores all of the children's conversations and the conversations of others who interact with the doll.[21]

---

[17] *See* Lee Moran, *Mattel Unveils Talking Hello Barbie Doll, Which Will Have Conversations with Kids,* N.Y. DAILY NEWS, http://www.nydailynews.com/life-style/mattel-unveils-barbie-talk-kids-article-1.2119732, *archived at* https://perma.cc/QLJ9-PHRQ (last updated Feb. 18, 2015, 8:18 AM).

[18] *See* James Vlahos, *Barbie Wants to Get to Know Your Child,* N.Y. TIMES MAG. (Sept. 16, 2015), http://www.nytimes.com/2015/09/20/magazine/barbie-wants-to-get-to-know-your-child.html, *archived at* https://perma.cc/BPV7-HDTD.

[19] *See* Ashlee Kieler, *Mattel Unveils Hello Barbie, a Doll That Can Hold a Conversation,* CONSUMERIST (Feb. 17, 2015), https://consumerist.com/2015/02/17/mattel-unveils-hello-barbie-a-doll-that-can-hold-a-conversation/, *archived at* https://perma.cc/24CB-PK44.

[20] *See id.*

[21] Mattel and ToyTalk responded to these concerns by confirming that the recorded conversations will not be used to advertise or market products to children, further nothing that parental consent is required to set up a Hello Barbie account. Also, interestingly, parents can listen to their child's recorded conversations and delete all recorded conversations. Additionally, ToyTalk states that it will only use the recordings to improve its speech recognition technology. *See Privacy Policy*, TOYTALK, https://www.toytalk.com/legal/privacy/, *archived at* https://perma.cc/Z8K8-2DRS (last

[11] Whether ToyTalk is controlling the object or its behaviors or listening to the people or other objects that its products interact with, these activities are important to lawyers investigating potential sources of relevant evidence in the litigation context. Perhaps a lawyer might send a subpoena to ToyTalk seeking the audio records from its client's Hello Barbie doll for use in a domestic abuse case. And Hello Barbie is not an outlier—there are a number of connected toys popping up on store shelves. It's rarely, if ever, explained to the consumer where the conversations these toys record and transmit are being stored, how that information is being used by the manufacturer or a partner company, and how it might be collected for use in litigation.

[12] Some enterprising companies, including several rent-to-own companies that ran into a bit of trouble with the FTC, put spyware (called Detective Mode) on their rental laptops that would turn on the built-in-cameras if the customer failed to make timely payments.[22] The spyware could also track the user's location, disable the computers, and add a fake software registration popup window that would take a user's registration information and transmit it back to the rental store, who would use it to track the renters to collect money.[23] Detective Mode also gathers data about whoever is using the computer, and transmits it to the software manufacturer every two minutes, who then sends the data to the rent-to-

updated Jan. 11, 2016). Mattel does seem to obtain data that it can use to market other products, and it does so with a parent's consent when they use Mattel's websites and apps. *See Mattel Online Privacy Statement and Children's Privacy Statement*, MATTEL, http://corporate.mattel.com/privacy-statement-shared.aspx, *archived at* https://perma.cc/QSV6-SXAV (last updated Apr. 9, 2014).

[22] *See* Press Release, Fed. Trade Comm., FTC Halts Computer Spying (Sept. 25, 2012), https://www.ftc.gov/news-events/press-releases/2012/09/ftc-halts-computer-spying, *archived at* https://perma.cc/R5XS-6DPR; *see also* David Kravets, *Rent-to-Own Laptops Secretly Photographed Users Having Sex, FTC Says*, WIRED (Sept. 25, 2012, 6:11 PM), http://www.wired.com/2012/09/laptop-rental-spyware-scandal/, *archived at* https://perma.cc/NQV4-6HQP.

[23] *See* Kravets, *supra* note 22.

own store.[24] Since the software collected private data including user names and passwords for e-mail accounts, social media websites, financial institutions, Social Security numbers, medical records, private e-mails, bank and credit card statements, along with webcam pictures of children, partially undressed individuals, and intimate activities at home, the FTC put a stop to the practice.[25] While these rental laptops are not considered an IoT object, similar spyware can be loaded on any object with a chip that includes a camera and access to the Internet and used to collect massively sensitive information.

### B. Wearable IoT Devices

[13] Wearable IoT devices include a wide range of medical devices and health and fitness products, including casual wearable fitness devices (like the Apple watch) and connected pacemakers and insulin pumps.[26] Wearable fitness devices, including smart watches and smart clothes, now monitor geolocation as well as heart rate, pulse, calorie consumption, sleep patterns, and other biological data.[27] Most wearable devices monitor very sensitive personal and health data. The devices constantly store data that users unconsciously create while going about their day. Wearables also transmit that data to the manufacturer and other entities for analysis and to share the information with the user so they can track their health

[24] *See* Complaint at 3–4, FTC v. Designerware, LLC., Kelly, & Koller (2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/09/120925designerwarecmpt.pdf, *archived at* https://perma.cc/96PJ-YVVP.

[25] *See id.*; *see also* Kravets, *supra* note 22.

[26] *See* ACCENTURE, *supra* note 4, at 3–4 (noting some reports indicate that over 28% of consumers will own wearable IoT technology by the end of 2016).

[27] *See, e.g.*, *Fitbit App*, FITBIT, https://www.fitbit.com/app, *archived at* https://perma.cc/5WER-PS9L (last visited Mar. 23, 2016).

and fitness over time.[28] Without a doubt, this data can be used in a court of law.

[14] The information wearable fitness and health devices collect can be highly relevant in determining, for example, where an individual was at a particular time and whether they have been "disabled" or injured as a result of a particular accident. A personal injury lawyer might be interested in the data collected from their client's wearable fitness device. For instance, the data obtained from a Fitbit device[29] has been used as evidence of an individual's diminished physical activity resulting from a work-related injury in a Canadian personal injury case.[30] The plaintiff used her Fitbit data to show that her post-injury activity levels were lower than the baseline for someone of the same age and profession to prove she deserved compensation for the injury.[31] With the help of a startup analytic company that aggregates Fitbit data and prepares analytical reports, her lawyers contrasted her personal data with the general population's health and wellness data (from other Fitbit devices) to make their case.[32]

[15] Prosecutors and defense counsel seeking incriminating or exculpatory evidence can also use wearable device data. In a case alleging rape in Pennsylvania, the Fitbit data contradicted the statements of the alleged victim by showing that at the time of the crime, she was awake and walking around, even though she claimed she was attacked while

[28] *See* Murray Grigo-McMahon, *My Data, Your Data, Our Data*, QLIK (July 6, 2015), http://global.qlik.com/us/blog/posts/murray-grigo-mcmahon/my-data-your-data-our-data?SourceID1=SocialChorus&__2hqwt_=2hqwt, *archived at* https://perma.cc/V479-N3CU.

[29] Fitbit is an extremely popular wearable fitness tracker.

[30] *See* Kate Crawford, *When Fitbit is the Expert Witness*, THE ATLANTIC (Nov. 19, 2014), http://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/, *archived at* https://perma.cc/AW5G-5NY2.

[31] *See id.*

[32] *See id.*

asleep.[33] She now faces misdemeanor charges because the Fitbit data contradicted her story.[34]

[16] Some wearables, like Google Glass, transmit location information, take photos and videos, and perform web searches. Imagine if a person who witnesses a crime while wearing this device took pictures of the perpetrator and the scene after the crime occurred.[35] Unlike surveillance technology, humans tend to look at something interesting or important. Technology like Google Glass might help them record valuable eye-witness evidence. The device may contain evidence like photos and geolocation information, along with time stamps, that police may use to investigate and prosecute crimes and civil litigants may use to pursue their cases.

[17] However, there are downsides to a person's voluntary collection of sensitive health information using a wearable device. Insurers and employers seeking to deny injury and disability claims can just as easily use wearable devices to support their own litigation claims and positions. It is generally seen as illegal for employers and insurers to force people to use the wearable devices.[36] But if individuals decide to collect this

[33] *See* Brett Hambright, *Woman Staged 'Rape' Scene with Knife, Vodka, Called 9-1-1, Police Say*, LANCASTER ONLINE (June 19, 2015, 2:57 PM), http://lancasteronline.com/news/local/woman-staged-rape-scene-with-knife-vodka-called--/article_9295bdbe-167c-11e5-b6eb-07d1288cc937.html, *archived at* https://perma.cc/YY5M-QEXF.

[34] *See* Kashmir Hill, *Fitbit Data Just Undermined a Woman's Rape Claim,* FUSION (June 29, 2015), http://fusion.net/story/158292/fitbit-data-just-undermined-a-womans-rape-claim/, *archived at* https://perma.cc/2J6W-BYAT.

[35] *See* Kashmir Hill, *Google Glass Will Be Incredible for the Courtroom*, FORBES (Mar. 15, 2013, 5:02 PM), http://www.forbes.com/sites/kashmirhill/2013/03/15/google-glass-will-be-incredible-for-the-courtroom/#604082cd36eb, *archived at* https://perma.cc/2QCU-NAYZ.

[36] *See* Adam Satariano, *Wear This Device So the Boss Knows You're Losing Weight*, BLOOMBERG (Aug. 21, 2014, 1:26 PM), http://www.bloomberg.com/news/articles/2014-

information on their own, device manufacturers or companies that store or report wearable device data might receive a subpoena for it, assuming the consumers don't have it.

[18] The fact that wearable device data may have evidentiary value should come as no surprise, given the fact that evidence from other self-tracking devices has already been used in court. Courts already use data from GPS devices and biking apps in cases involving bike accidents.[37] Police routinely use surveillance technology like Automatic License Plate Readers (ALPR) mounted on police cars, or on objects like road signs and bridges, to photograph thousands of plates per minute and track motorist movements.[38] Private companies also collect license plate photos and geotagged images and sell that data to law enforcement, insurers, and financial institutions.[39] They consider this analogous to taking photographs in public and disseminating the information, an activity protected by the First Amendment.[40] This is one part of a larger trend toward surveillance of private citizens' activities. While this type of

08-21/wear-this-device-so-the-boss-knows-you-re-losing-weight, *archived at* https://perma.cc/GS3Y-KXF6.

[37] *See* Patrick Brady, *Prosecution Rest in LA Road Rage Rase. Defense Will Call Witnesses Monday*, VELONEWS (last updated Nov. 3, 2009, 7:00 PM), http://velonews.competitor.com/2009/10/news/prosecution-rest-in-la-road-rage-case-defense-will-call-witnesses-monday_99537, *archived at* https://perma.cc/87G9-KLSP.

[38] *See* Conor Friedersdorf, *An Unprecedented Threat to Privacy*, THE ATLANTIC (Jan. 27, 2016), http://www.theatlantic.com/politics/archive/2016/01/vigilant-solutions-surveillance/427047/, *archived at* https://perma.cc/NL4V-AJKA (discussing how one private company has taken approximately 2.2 billion license-plate photos to date, and each month it captures and permanently stores nearly 80 million more geotagged images).

[39] *See id.*

[40] *See* David Sirota, *Companies Test Their First Amendment Right to Track you*, OR. LIVE, http://www.oregonlive.com/opinion/index.ssf/2014/03/companies_test_their_first_ame.html, *archived at* https://perma.cc/VZ8R-K7QS (last updated Mar. 8, 2014, 7:10 AM).

surveillance usually occurs without consent, wearable tracking is voluntary.

[19] One issue raised by wearable evidence involves the reliability of the data and the analyses performed on it. The software that analyzes wearable data interprets the wearer's daily activities and compares that data to predetermined baselines and standards set by the manufacturer. For example, Fitbit monitors sleep patterns, decides how many hours a user sleeps, and determines the quality and efficiency of that sleep.[41] The wearer is compared to the "average" sleeper (as determined by the manufacturer's algorithm).[42] That information might be useful for an employer defending itself against a worker's compensation claim, particularly if the sleep analysis reveals that the worker was considered "sleep deprived" by the data analysis at the time of the accident. So regardless of her personal optimal sleep duration or the outside forces that might have impacted her sleep the night before the accident occurred, she would be categorized and measured against a population baseline.

[20] Other wearable devices collect different data, function differently, and use different algorithms and standards to analyze data and report trends and health information in comparison to the general population.[43] All of this means that before wearable evidence is used in a case, you need to understand what it means and the limitations inherent in the analysis of that data. This information should be clearly explained to the fact finder

[41] *See What Should I Know About Sleep Tracking?*, FITBIT, https://help.fitbit.com/articles/en_US/Help_article/Sleep-tracking-FAQs, *archived at* https://perma.cc/KB2D-MZMW (last updated Mar. 7, 2016).

[42] *See id.*

[43] The wearable fitness device market includes Nike Fuelband, Fitbit, Withings Pulse, and Jawbone Up, among others. A number of companies have also developed fitness apps that interact with these wearable devices and collect the user data they create. Fitbit lists over 30 apps that are compatible with the Fitbit device. *See Compatible Apps*, FITBIT, https://www.fitbit.com/partnership, *archived at* https://perma.cc/P2L9-TNE4 (last visited Mar. 25, 2016).

by someone who knows the IoT device that collected the data and the analytic method or methods it uses to interpret that data. Perhaps the IoT revolution will give rise to a whole new class of "experts" who interpret wearables data and the analytics engines in a courtroom setting.

### C. Connected Cars

[21] Another category of IoT technology relates to connected transportation. Today, many cars have sophisticated software that connect the user to many remotely managed features including real-time navigation, mapped points-of-interest, dash-based Internet search, streaming music, and mobile device app connectivity.[44] IoT implicates a wide variety of technologies involved with running and monitoring connected cars, including connected control systems, Event Data Recorders (EDRs), and other vehicle telematics.[45] Vehicle control software may use proximity sensors to identify collision risks and automatically engage the brake, survey blind spots and report objects, and park a vehicle without driver assistance. Automakers are turning vehicles into smartphones using connection technology that controls the entertainment and navigation systems, enables phone calls, and provides a Wi-Fi hotspot. Further, a number of well-know tech companies are currently testing driverless cars and intend to offer self-driving cars in the near future.[46] These cars will be connected to the Internet and they will

[44] *See, e.g.*, *Cisco Connected Transportation*, http://www.cisco.com/c/en/us/solutions/industries/transportation.html, *archived at* https://perma.cc/548E-TPXF (last visited March 25, 2016).

[45] An EDR is "a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event (e.g., vehicle speed vs. time) or during a crash event . . . intended for retrieval after the crash event." 49 C.F.R. § 563.5 (2015). Telematics refers to data collection transmission, and processing technologies for use in vehicles.

[46] *See* Alice Truong, *Tesla Just Transformed the Model S into a Nearly Driverless Car*, QUARTZ (Oct. 14, 2015), http://qz.com/524400/tesla-just-transformed-the-model-s-into-a-nearly-driverless-car/, *archived at* https://perma.cc/J439-T5JZ; Cadie Thompson, *There's One Big Difference Between Google and Tesla's Self-driving Car Technology*, TECH INSIDER (Dec. 5, 2015, 12:00 PM), http://www.techinsider.io/difference-between-google-

transmit all kinds of data relating to the vehicle and its passengers' activities.

[22] Particularly in light of the Volkswagen emissions scandal,[47] the connected control systems on vehicles are of great interest to the public and regulatory bodies. Additionally, an insurance carrier might seek records reflecting the information an auto manufacturer collects through a connection with an in-dash entertainment system and the data relating to car speed and breaking that resides in the vehicle control system. Was the driver checking her email while driving 70 miles an hour before she rear-ended another car? And a class action lawyer might find the data housed on EDRs useful in a class action lawsuit relating to certain safety issues involving the physical components of vehicles or the software that runs them.

[23] Some vehicles have safety features that include automated calls in case of emergencies, and in at least one reported incident, a hit and run accident was foiled when the fleeing driver's car called the police after impact.[48] The car synced to the driver's phone using Bluetooth, and because the emergency call feature was enabled, it gave police the vehicle's GPS location and opened the line so the driver could talk with

---

and-tesla-driverless-cars-2015-12, *archived at* https://perma.cc/RED9-CQTZ; Feann Torr, *Next-gen Audi A8 Drives Better Than You,* MOTORING (Oct. 22, 2014), http://www.motoring.com.au/next-gen-audi-a8-drives-better-than-you-46963/, *archived at* https://perma.cc/UFL4-76FG; Tom Risen, *Report: Uber, Lyft Poised to Win on Driverless Cars*, U.S. NEWS & WORLD REP. (Nov. 13, 2015, 4:05 PM), http://www.usnews.com/news/articles/2015/11/13/report-uber-lyft-poised-to-win-on-driverless-cars, *archived at* https://perma.cc/3HPV-8RJ9.

[47] *See* Russell Hotten, *Volkswagen: The Scandal Explained*, BBC NEWS (Dec. 10, 2015), http://www.bbc.com/news/business-34324772, *archived at* https://perma.cc/8YKM-6W5W.

[48] *See* Kashmir Hill, *Florida Woman's Car Calls Police After She Flees the Scene of an Accident*, FUSION (Dec. 7 2015, 11:46 AM), http://fusion.net/story/242193/womans-car-calls-police/, *archived at* https://perma.cc/JDE6-SDST.

the police.[49] The owner told the police that her car was not in an accident when connected, but the dents in the front of her car and her airbags told a different story when the police showed up at her house later.[50]

[24] At least one rental car agency is already putting cameras in navigational devices installed in its fleet of cars, and the user cannot disable the camera.[51] While the agency reports that these cameras are not currently optional, they are clearly moving towards the day when customers (and the entire interior of a car) will be visible to their representatives if a service call is made using the navigational device.[52]

## IV. E-DISCOVERY OF IOT INFORMATION

[25] Lawyers and clients should prepare for IoT-related e-discovery issues. IoT objects will present many challenges in the e-Discovery context. There are limitations on wearable devices and other IoT objects and the information they collect, however, the technology is becoming more sophisticated, accessible, and shareable every day. And when information is shared among multiple objects—a watch, a smartphone and a cloud computing system—the preservation issues are complex. Also, some IoT data is ephemeral and never really stored for future use or access. The Federal Rules of Civil Procedure provide some flexible guidance for dealing with this technical revolution, and counsel against "a limiting or precise definition of electronically stored information."[53] Yet companies that store data from IoT devices will need to develop processes

[49] *See id.*

[50] *See id.*

[51] *See* Kashmir Hill, *Hertz Puts Cameras in Its Rental Cars, Says It Has No Plans to Use Them*, FUSION (Mar. 13, 2015, 1:46 PM), http://fusion.net/story/61741/hertz-cameras-in-rental-cars/, *archived at* https://perma.cc/85TF-DDUM.

[52] *See id.*

[53] FED. R. CIV. PRO. 34, advisory committee's note on 2006 amendments.

for preserving, collecting, and producing it when the duty arises—whether it's the consumer's duty or their own.

[26] The legal regimes that govern the capture, processing, use, and ownership of object data are important when determining whether we—or our clients—have a duty to protect data generated from IoT activities (keep it secure and confidential) or preserve and produce it in a litigation. Often, consumers will expect that their wearable device data is "off limits" and they are surprised to learn that it can be used in certain types of cases. The sooner litigators identify the important IoT data clients and their customers generate and the objects they interact with everyday, the better off everyone will be when evaluating the legal risks and obligations to secure and produce that information.

[27] Additionally, as IoT finds its way into the courtroom, judges will be asked to analyze the complex possession, custody, and control issues encountered in the IoT context. These questions may involve an analysis of the relative cost and burden associated with owner focused or manufacturer focused production options. For example, if an owner must jailbreak her device and hire an expensive expert to collect data off her wearable device, but the manufacturer can export her data with relative ease, courts should consider such practical realities when deciding their relative obligations. Moreover, access controls, privacy restrictions, and contractual obligations play a role in determining the appropriate process for engaging in e-discovery of IoT data.

[28] One of the practical problems relating to collection of IoT information is that device manufacturers each collect data in their own way. And the analytic platforms that collect and aggregate IoT data do the same thing. Raw data residing on IoT objects may not be preserved or collected without undertaking significant efforts at a significant cost. The manufacturers don't build these objects with the purpose of making it easy to collect information from them directly. This makes it particularly difficult to develop standard processes for preserving, collecting, reviewing, and producing information from a wide variety of IoT objects using their APIs or built in data reporting and download features. It also

makes it hard to aggregate data from different devices and standardize it to obtain big data metrics using data collected from all wearable devices of a particular class. Given these issues, the cost associated with using this type of data could be prohibitive, given the relatively lower value of a case and the damages at stake. This is a prime area in which companies and e-discovery vendors can innovate and create a strong market for flexible services and solutions involving IoT device data.

[29] Undoubtedly, more lawsuits involving IoT data are coming, as more lawyers and litigants realize that the data is discoverable, relevant, and useful as evidence that can support their case. Litigators and clients should understand how IoT objects work, what information they collect, where it is stored, how long it is stored, and who is obliged to keep it safe. Only after we understand how the system works, can we make strategic decisions about legal risks, e-discovery options and obligations, and appropriate use of IoT data in court. It will be interesting to see how the market responds to the challenges that will arise when parties start engaging in IoT discovery.

## V. IoT Object As Witness

[30] As wearables and other IoT objects find their way into the courtroom, litigators must figure out how we will use IoT information as "witness" evidence. Did we ever imagine that the objects gathering information about us could be used against us? Will judges and juries treat it like forensic evidence, and give it the same weight and credibility as scientific analysis or the results reported by an expert witness? Not unlike scientific researchers or forensic experts, wearable technologies collect data, interpret it, and reflect it in reports that provide information about the user activity and experience.

[31] It will be particularly interesting to see what happens when a witness's sensory experiences (sight, sound, taste, etc.) clash with the "experience" reported by their wearable device and how the fact finder reconciles these competing stories. For example, if a biker testifies that they were traveling down a hill towards an intersection at about 15 miles

per hour, but their wearable device or Strava[54] app reports the speed down the slope at 25 (due to a complicated three-dimensional GPS reading and reporting algorithms), which "witness" will the jury credit more? Both systems for reporting experiences are fallible and fraught with errors. But if litigators prioritize IoT data-driven evidence over eyewitness statements or expert analysis, then we must ensure that the algorithms used to analyze IoT data are understood and their imperfections are disclosed. As one commentator noted, if we think of devices as partial witnesses, we must understand that they carry biases and have a worldview, based on their relationship with their environment.[55]

[32] There is a significant risk that IoT object information, for instance, the Fitbit data and its sleep analysis,[56] would carry more evidentiary weight than the owner's own experience and view of her sleep patterns or alertness at the time an injury occurred. As with forensics results, there is a significant risk that judges and jurors will conclude that device data doesn't lie or have an imperfect memory. Yet there is an interpretive activity lurking behind the scene. When wearable object data is collected and interpreted by analytics companies using proprietary algorithms, counsel, judges and juries will need to understand what's happening under the hood, whether the results reported are reliable, and what evidentiary weight they should be given. The interpretive tools used to report IoT data are often highly subjective or an imperfect fit for a number of users because of their crude analysis methods or the individual's health status and biology. This is but one area where possibilities are far ahead of the law on witness-style testimony from things connected the Internet.

[54] Strava is a running and cycling GPS tracker. *See generally* STRAVA, https://www.strava.com/about, *archived at* https://perma.cc/9F99-EWPY (last visited Mar. 21, 2016).

[55] *See* Crawford, *supra* note 30.

[56] *See What Should I Know About Sleep Tracking?*, *supra* note 41.

[33] Only time will tell whether this type of IoT information is seen as objective and unbiased evidence in the courtroom. If we can't demonstrate that IoT evidence meets the requirements for introduction of scientific or forensic evidence, then it may be excluded.[57] If introduced, it may be given too much weight in light of its significant limitations. A balanced approach is needed.

[34] Courts will also have to figure out how the Fifth Amendment protects the right against self-incrimination when the incriminating evidence involves user data created by an IoT object. And the Sixth Amendment provides the Constitutional right to confront a witness that will provide evidence against the accused in a criminal prosecution.[58] How would a witness confront her wearable device or the companies that think they know the best way to interpret the data it collects? This raises fundamental philosophical questions regarding the witness who must be available for "confrontation." Is it you, your device, the manufacturer, the service provider that collects and analyzes your data, or the company that provides the algorithms used to interpret it? The case law is going to be messy and inconsistent as courts start considering the obstacles presented by use of IoT evidence in the courtroom and sorting the Constitutional issues out.

[35] Additionally, as more IoT objects are used in litigations, people's relationships with their wearables are likely to change. How will they react after learning that the connected IoT objects they interact with can be used as an involuntary informant? Perhaps the day is coming when eyewitness testimony will become almost irrelevant and will be replaced by the information our objects provide about our location, health, conscious state, and activities at any given time. But while IoT can reveal truths, those truths must be understood in context, in all their fallible or limited glory.

[57] *See* FED. R. EVID. 702.

[58] *See* U.S. CONST. amend. VI.

## VI. LITIGATING IN AN IOT WORLD

[36] Some have called IoT a third major revolution—one built on the industrial revolution and the Internet revolution.[59] Lawyers and their clients are becoming more reliant on IoT to manage, monitor, and control their objects, interact, and work on the substantive aspects of their job. Regardless of the source, the information that IoT objects collect and share provide litigators rich new evidence stores that should be explored to find interesting information that impacts their case.

[37] A tech-savvy lawyer knows how to get the right evidence in the right format from her client or opponent. The fact that IoT raises a number of novel and interesting legal issues and practical complexities means that tech-savvy lawyers, with a good grasp of the basic issues, will be well positioned to provide thoughtful and constructive advice. This guidebook provides some basic information regarding IoT technologies, legal issues, and practical concerns that should be considered. But it needs to be applied to the real world, for each client and case, and in the context of each connected collection of objects, companies, and people. The IoT movement is your opportunity to continue your self-education journey, and learn more about the implications of IoT on lawyering in the Information Age.

[59] *See* Harish Nivas, *How Internet of Things is the Next Big Industrial Revolution*, IOTWORM (Jan. 23, 2016), http://iotworm.com/internet-of-things-next-big-industrial-revolution/, *archived at* https://perma.cc/JD9Y-T64S.