the IoT:

WHAT IS THE INTERNET OF THINGS?

The term "Internet of Things" (IoT) refers to the internetworking of a wide variety of objects embedded with electronics, software, sensors, actuators, and connectivity that enables these objects to generate, collect, and exchange data. While each object is separately and uniquely identifiable, what sets the IoT apart from a mere multiplicity of objects is the fact that the objects are capable of operating together through existing internet infrastructure. The interconnectivity of the IoT allows objects to be sensed or controlled remotely across networks, creating opportunities for more direct integration of the physical world into computer-based systems.

Gartner[1] points to the rapid growth of the IoT, noting that in 2017 approximately 8.4 billion objects were expected to be in use, up 31 percent from 2016. Gartner, in that estimate, does not include smartphones, tablets, and computers, of which there are many more billion units. Expert predictions of the breadth of the IoT by the year 2020 vary widely, ranging between 20.8 billion and 30.7 billion such devices. Even if the growth turns out to be less rapid than many expect, the extent to which our lives will be affected by interconnected devices will surely be enormous, and the associated legal issues promise to engage a greater and greater portion of the time of legal practitioners of all sorts.

LIVING IN AN INTERCONNECTED WORLD

The explosion of internet-connected devices has affected all of our lives in one way or another. In order to get a sense of the many ways we come into contact with such devices, we can usefully distinguish among consumer, business, and infrastructure applications.

Consumer applications include connected entertainment, car, and smart home devices such as washer/dryers, refrigerators/freezers, ovens, robotic vacuums, heating systems, or air purifiers that use Wi-Fi for remote monitoring. Smart home technology also includes devices that provide assistance for disabled and elderly persons, including monitors for seizures or falls, and other kinds of connected health devices. Recent years have seen an enormous increase in the prevalence of wearable technology, such as Fitbit or Apple Watch, and "quantified self"

Ronald J. Hedges is a member of Dentons' Litigation and Dispute Resolution practice group. He has extensive experience in e-discovery and in the management of complex litigation and has served as a special master, arbitrator and mediator. He also consults on management and discovery of electronically stored information (ESI). He was a U.S. Magistrate Judge from 1986 to 2007 and is the principal author of the third edition of the Federal Judicial Center's *Pocket Guide for Judges on Discovery of Electronic Information*, available under "publications" at the FJC website. Website: www.dentons.com/en/ronald-hedges. LinkedIn: www.linkedin.com/in/ron-hedges-710421126.

What Is It, What Can Happen With It, and What Can Be Done When Something Happens

By Ronald J. Hedges and Kevin F. Ryan

technologies (data acquisition on aspects of a person's daily life in terms of food consumption or exercise, physical states such as heart rate, mood, arousal, blood oxygen levels, and mental or physical performance). Automobiles now have built-in, computer-connected sensors that tell the operator to brake or get back into his or her lane, and we are not far from the day when highways will be filled with self-controlled vehicles requiring minimal operator input.

Some devices straddle the line between consumer and business application. For example, cameras and audio devices can stream live feeds of everything from babies in the nursery, to building and property perimeters, to conferences, to wild animals in remote regions of the world.

Business (or enterprise) applications include various devices aimed at determining and responding to consumer preferences and linking marketing to personal devices via text messaging or other forms of communication. Also included are various technologies used to track consumer responses, such as conversion tracking, drop-off rate, click-through rate, and interaction rate. The IoT also includes network control and management of manufacturing equipment, permitting greater efficiency in the development of new products, dynamic response to product demands, asset management, and health and safety management. Finally, a wide range of health care applications has emerged, connecting patients and data about them with medical personnel many miles away.

Infrastructure management applications include technologies that permit monitoring and controlling bridges, railway tracks, wind farms, and other structures and facilities. A large class of cyber-physical systems have emerged, including smart grids, virtual power plants, intelligent transportation (computer-operated train systems, for example), and smart cities. IoT infrastructure can be used to observe conditions that can compromise safety and security, to schedule repair and maintenance activities efficiently, and to assist firefighters, soldiers, and others in search and rescue or military operations.

PROBLEMS THAT MIGHT ARISE WITH INTERCONNECTED DEVICES

Given this proliferation of interconnected devices, what kinds of legal problems can we expect to arise? We suggest potential problems can be of several sorts: they can be related to (1) privacy concerns, (2) security concerns, (3) investigation and criminal matters, or (4) personal injury and other sorts of civil litigation. In this article, we focus solely on litigation issues raised by the IoT. But a brief tour of other sorts of problems will give the reader a sense of the tremendous breadth of legal issues that will soon emerge (if they have not already done so).

The devices and networks in the IoT contain and transmit a huge amount of personal data, information that the average person would consider private. Medical and health devices contain information about activity, heart rate, diet, and so forth; smart homes know when residents were at home and when they were not; cameras

Kevin F. Ryan, (kryan@mcba.org) is Executive Director of the Monroe County Bar Association. Prior to coming to the MCBA, he was the Director of Education and Communication at the Vermont Bar Association for 15 years. He has also taught on the faculties of the Vermont Law School, Norwich University, the University of Denver, Regis University, and others. He has presented numerous CLE programs on subjects ranging from legal ethics to technology and law office management. He holds a graduate degree in political science from Princeton University and a JD from the University of Denver Sturm College of Law. He has also been a visiting scholar at Harvard Law School. Website: www.mcba.org. Facebook: www.facebook.com/mcbany/. Twitter: @MCBA_ny. LinkedIn: https://www.linkedin.com/groups/2449682/profile.

contain images, some of which may be compromising, and the metadata about those images; business applications know consumers' purchasing habits and their responsiveness to particular sorts of messages. It remains to be seen what information about an individual might be held and distributed within smart cities. We may be living in an age when the boundaries of privacy are shifting, but the amount of information about a person that will be moving around the IoT is truly staggering and guaranteed to generate major privacy concerns.

With all that data floating around on networks, security becomes a critical issue. The recent spate of security breaches, from Equifax to hospitals in several states and nations to the National Security Agency, illustrates the susceptibility of even tightly secured networks to the work of malicious hackers. As more information about individuals finds its way into the IoT, potential for such security breaches increases.

Obviously, the devices and networks of the IoT contain personal information that might reveal aspects of a person's condition or behavior, and therefore become

the target of investigatory and criminal proceedings. An Apple Watch knows how far someone walked yesterday and what their heart rate was and that data has entered the network. A cell phone contains even more information about a person's movements. A smart home knows not only when a resident was there but also what lights were on and whether the security system was engaged. As new devices and interconnections emerge, the opportunities to investigate aspects of someone's life increase exponentially. Lawyers and judges are already wrestling with determining what sorts of data from what sources can be sought in criminal proceedings and considering the ways the traditional rules may need to change to take into account the new world of the IoT.

LITIGATION

With the above as background, let's assume that "X" had just left her office and was driving home in her new-model SUV. She decided that, because the weather had become chilly, she would increase the temperature in her home by four degrees. She instructed the smart thermostat in the home to accomplish this with a smart phone app that controlled the thermostat. The phone was connected through a Bluebooth device to her SUV and from the SUV to a Wi-Fi. Thirty minutes after the instruction to the thermostat she arrived at her home. It was aflame and the fire department had arrived and was at work, having been alerted to smoke and flames coming from the home by a neighbor. By the time the fire was extinguished, the home and its contents were a total loss.

X immediately thought that something was wrong and so she consulted an attorney about possible litigation. The attorney agreed that something seemed to have gone wrong but told X that he would have to undertake an investigation before he could commence a civil action. The attorney explained that he would have to contact whoever was in the likely chain of causal acts, ask for whatever records might be available, and consult with an expert to review the records and see what happened. (Of course, he put whoever he contacted on notice of possible litigation and requested that all records be preserved.)

As a result of the investigation, the attorney became satisfied that there was sufficient evidence that the app "miscommunicated" the temperature change to the thermostat and that the miscommunication caused a temperature rise that destroyed the home heating system and started the fire. The attorney was also satisfied that the thermostat should have recognized the miscommunication and prevented the rise of temperature to a dangerous level. On the first anniversary of the fire, X's attorney filed a diversity action in United States district court, naming the manufacturers of both devices as defendants and asserting products liability claims. He also asserted negligence claims, not being convinced that products liability claims would suffice.

After the defendants unsuccessfully moved to dismiss the complaint on *Twombly*/*Iqbal* grounds, they filed answers. In the answers the defendants asserted, among other things, that X was herself responsible at least in part for the fire because she had not completed installation of either the app or the thermostat. Had she followed all the prompts on installation she could have directed the app and the thermostat to "cap" temperature change. In any event, the thermostat could have been enabled to detect smoke and fire in the home and to send a signal to the local fire department when it did so. Moreover, the defendants asserted third-party claims against every other entity in the causal chain because the evidence the app manufacturer gathered from its records appeared to show that X's instruction somehow became "garbled" in transit to the thermostat.

Once the defendants answered, the parties conducted a Rule 26(f) conference to prepare a joint discovery plan. Discovery disputes arose immediately. These included:

1. X's attorney learned that the defendant manufacturers had not instituted a litigation hold on receipt of his preservation letter. They took the position that the letter was insufficient to put them on notice of imminent litigation. Instead, holds were implemented on receipt of summonses.

2. X's attorney advised the defendants that he intended to demand production of, among other things, the source codes for the app and the thermostat so that his expert could determine why the devices failed. In response, the manufacturer of the app advised that the source codes were irrelevant and that, in any event, the source codes had been modified six months after the fire and pre-modification codes had not been retained. Moreover, the source codes would have to be subpoenaed because these were developed by independent contractors in other states. Finally, both manufacturers took the position that all source codes were trade secrets and proprietary and would not be turned over absent a protective order that restricted access to only one expert.

DISCOVERY-RELATED ISSUES

Let's step back from our hypothetical and think about the issues presented for ultimate resolution. First, as to causes of action and defenses:

1. Rule 11 imposes an obligation on a putative plaintiff's attorney to conduct an adequate investigation into the facts and controlling law prior to signing a pleading. What might "adequate" mean in the context of an IoT action? However "adequate" might be defined, it will likely be necessary for the attorney to retain one or more consultants to assist him before the commencement of litigation. Why? The attorney will need to understand, among other things, the operation of the devices in issue, the interaction between the devices, and existing safeguards against data breach and untoward consequences.

2. The plaintiff in our hypothetical asserted cause of action sounding in both strict liability and negligence, and the defendants have alleged that X was herself negligent. The defendants also asserted third-party claims against (presumably) Bluetooth and the manufacturer of the SUV. The IoT may give rise to a multi-party action that may culminate in an allocation of fault between all parties.

3. Given the nature of the IoT and, specifically, the development and implementation of the app and devices in issue, both fact and expert testimony will be necessary to allocate liability. The latter will require *Daubert*- or *Frye*-qualified expert opinions.

Then, as to discovery:

1. Discovery in an IoT-related action will likely involve large volumes, and perhaps varieties, of electronically stored information (ESI). That ESI will have to be collected, searched and analyzed in defense of asserted causes and actions and, to at least some degree, produced. That production will itself have to be searched and analyzed by the receiving party. These various tasks will almost certainly require the assistance of nonparty consultants. Without that assistance, no attorney may understand the "ins and outs" of interconnected devices.

2. Large volumes and varieties of ESI may give rise to concern about proportionality under Rule 26(b)(1). Assuming that a party asserts that a discovery request is not proportional to the needs of the action, what proofs should that party be prepared to offer and what witness or witnesses will that party rely on to do so?

3. "[P]ossession, custody or control" of ESI for Rule 34(a)(1) might well be a recurring question in IoT actions. As in our hypothetical, third-party vendors or consultants might maintain ESI that is relevant to a claim or defense. If so, can a requesting party demonstrate that a responding party has some tie to a third party sufficient to require that party to make a production? If not, the requesting party will presumably have to subpoena the third party. Resolution of "control" is likely to be a fact-intensive undertaking.

4. Requests for discovery in an IoT action may well encompass arguments that the ESI sought is proprietary and that the discovery not be had. This raises the possible need for protective orders under Rule 26(c) and limitation of access to the proprietary ESI.

5. As with every action involving ESI, there is the possibility that at least some ESI may have been lost. Any loss may lead to proceedings unrelated to the merits.

CONCLUSION

We may be entering a brave new world of complexity in civil litigation because of the IoT. That complexity may require attorneys to devote additional time and resources to understand the ways in which the IoT works, thus fulfilling the duty of competence under Rule of Professional Conduct 1.1.

1. Gartner, Inc. is a research and advisory firm providing information-technology-related insight for IT and other business leaders located across the world.

SOURCES

- E. Corken, "Current Issues Regarding Possession, Custody or Control," 16 DDEE 426 (2016).H.B. Dixon, Jr., "The Wonderful and Scary Internet of Things," Judges' Journal 36 (Summer 2017).
- "The Smart Home Checklist" (Online Trust Alliance), at https://otalliance.org/system/files/files/initiative/documents/ota_smarthome_check_list.pdf.
- The Sedona Conference Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control," 17 Sedona Conf. J. 469 (2016).
- United States Department of Homeland Security, "Strategic Principles for Securing the Internet of Things (IoT)" (Nov. 15, 2016), at https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf.
- Press Release, Gartner, Inc., Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, at https://www.gartner.com/newsroom/id/3598917.
- Amy Nordrum, "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated," IEEE, Aug. 18, 2016, https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated.