The Wonderful and Scary Internet of Things!

By Judge Herbert B. Dixon Jr.

This is a follow-up to the technology column in the previous issue of *The Judges' Journal* concerning the possibility that your Internet device might be spying on you.[1] For the most part, that article was referring to the Internet of Things (IoT), a shorthand reference to devices (things) that use technology to communicate wirelessly between themselves, either storing data, executing preprogrammed instructions, or providing information to human users.[2] The IoT offers wonderful conveniences and benefits. However, for those who are apprehensive of technology, this article may confirm the worst of your "I told you so" fears as we contrast the vulnerabilities brought on by the new conveniences. As we make these comparisons, I invite you to consider the lawsuits and courtroom dynamics likely to result from the situations described below.

Revenge of the Garage Door Opener Manufacturer

Imagine a consumer who purchases a garage door opener that enables her to control the door to her home garage from anywhere in the world. This capability exists because the garage door opener is connected to the Internet through the consumer's home Wi-Fi, which allows the consumer to communicate with the device through an app on her smartphone. Although the Internet provides worldwide access to the device, there will not be a frequent need for the consumer to operate the device other than when she is leaving or approaching the garage, unless the consumer wants to double-check the status of the garage door while she is on vacation. Yes, there can be a wonderful uplift to your psychological well-being when you have the digital capability to confirm from anywhere in the world that your garage door is safely closed.

Next, imagine the consumer's disappointment when the device does not work reliably. Because of this negative experience, the consumer submits a "poor" rating of the device to the online merchandiser, stating "Junk—DO NOT WASTE YOUR MONEY—iPhone app is a piece of junk, crashes constantly, start-up company that obviously has not performed proper quality assurance tests on their products."[3] As you might expect, the poor rating posted by the consumer infuriated the manufacturer, who then took matters into his own hands. In the words of techies, the manufacturer "bricked" the device, which means he went online and permanently disabled the garage door opener. The manufacturer notified the consumer that the device was being denied server connection and further stated that the consumer's only option was to return the device to the retailer for a refund. In other words, "take that" for the poor rating you gave my invention. Wow! The repossession of an automobile after a consumer fails to pay the monthly note seems mild when compared with this manufacturer's online self-help solution. In a nanosecond, reaching from cyberspace, the manufacturer effectively repossessed the device because of the consumer's complaint.

The Mischievous Autonomous Vehicle Hacker

First, by way of background, an autonomous vehicle, also known as a driverless vehicle, operates using technologies that include onboard and cloud computers and software, laser and optical guidance systems to avoid collisions and obey traffic signals, constantly updated data concerning traffic and road conditions, GPS, and much more. Second, some in the automotive industry have predicted the mass production and availability of level-five fully autonomous

vehicles without steering wheel or pedals by 2025, reaching various incremental milestones along the way by 2019 and 2021. Third, before you become terrified about the hacking vulnerability of an autonomous vehicle, be assured there is aggressive and constant research in the industry to build antihacking technology into these vehicles to stay ahead of any possible mischievous hacker.[4]

Imagine a consumer who has purchased a level-five fully autonomous vehicle and has been enjoying the benefits of the vehicle: (1) driving the owner to work and going back home to park in the owner's garage until time for the after-work pick-up; (2) driving the owner to the airport, going back home to park in the owner's garage, and returning to the airport on command when the owner's flight returns home; and (3) operating as the owner's personal chauffeur service for all local and some long-distance transportation needs. Obviously, this is the wonderful part of the benefits of being a level-five fully autonomous vehicle owner.

Now, consider the scary part. Is it possible that a disgruntled or former ex-suitor, scorned acquaintance, business competitor or associate, or enemy might either have the personal knowhow or hire someone with sophisticated skills to hack the autonomous vehicle to (1) disable the starting mechanism, (2) disable all aspects of the collision avoidance systems, (3) cause the vehicle to unexpectedly accelerate and maintain a high speed, (4) shut down the vehicle once it reaches highway speeds, or (5) take over the vehicle's operations?

Any of these possibilities would be frustrating, at a minimum, or frightening to an owner or vehicle passenger. Considering the possibility the vehicle may be used for car or ride sharing (e.g., Lyft, Uber, or Zipcar), the mischievous activity would affect more than just a single owner. Is that scary enough for you?

Remote Management and Monitoring of Patients and Medical Equipment

The process of remote management and monitoring of patients and medical equipment is occurring with increasing frequency. This includes control of infusion pumps to release patient medication, including insulin pump systems to manage blood glucose levels; implantable cardioverter defibrillators that deliver shocks to a patient who shows signs of going into cardiac arrest; refrigeration systems to preserve blood and pharmaceuticals; and CT scanning systems to set patient radiation exposure limits and amounts.[5] Nevertheless, with the wonderful convenience of Internet access to manage the interaction between patients, equipment, and medication, there are life-threatening vulnerabilities to malicious hacking. One example of the concern about the hacking of medical equipment is demonstrated where doctors for former Vice President Dick Cheney ordered the wireless functionality of his heart implant disabled due to fears it might be hacked in an assassination attempt.[6]

At one time, there was a concern that medical equipment was more vulnerable to hacking than other Internet-connected devices because (1) medical software tended to be older and more vulnerable than other consumer technologies and (2) updating medical equipment software might adversely affect the Food and Drug Administration (FDA) approval of the equipment. As more devices were networked, i.e., connected to the Internet with advancement in IoT technologies, that concern was amplified.[7] Fortunately, there has been progress addressing these concerns. The FDA now includes cybersecurity protection as one of many evaluation criteria for approval of medical devices.[8]

Video Surveillance and Other Devices on the IoT

The IoT provides a convenient way for individuals using a computer to keep an eye on the inside and outside of their homes from any location with Internet access. This includes using one's office computer or personal laptop, and a range of smartphones, tablets, and other mobile devices. This ability to monitor one's home allows activities ranging from a resident checking from within the home on the baby's activity in the nursery, to monitoring activity around the home that might include ordinary front door visitors or potential burglars. Even with the wonderful convenience and peace of mind this capability provides to the homeowner, there are vulnerabilities. Some video surveillance manufacturers have not required consumers to change the default ID and adopt secure passwords before placing the equipment in operation. How often have you maintained the user ID "admin" and the password "password" or "123456"? Because of a lack of diligence by the manufacturer or consumer, hackers have been able to find and surreptitiously view live video of other individuals' homes, offices, nurseries, and other locations, starting with a random Internet search, e.g., for baby monitors.[9]

There is an additional and heightened vulnerability to webcams—an instance in which a hacker uses the device to launch a "Distributed Denial of Service" (DDoS) attack. A DDoS attack occurs when a hacker uses millions of IoT devices (DVDs, refrigerators, webcams, thermostats, computers, etc.) whose unchanged, default IDs and passwords have been compromised to overwhelm and shut down a targeted computer or computer system. One example of a DDoS attack is the October 2016 massive Internet outage along the East Coast of the United States.[10] Another example is the largest-known DDoS attack when the British Broadcasting Company suffered a massive outage on New Year's Eve of 2015 by a group known as New World Hacking, which on the same day also hacked the Donald Trump campaign.[11]

Judge Herbert B. Dixon Jr., a senior judge on the Superior Court of the District of Columbia, is a member of the ABA Board of Governors and a former chair of the National Conference of State Trial Judges. He can be reached at Herbert.Dixon@dcsc.gov. Follow Judge Dixon on Twitter @Jhbdixon.

Tattletale Wearable Devices and Personal Assistants

Another wonderful benefit of the IoT involves so-called wearable devices that track the number of steps per day, pulse rate, number of hours we sleep, and many other data points to advise us if we are engaged in a healthy lifestyle. These wonderful benefits may not be what a Connecticut man was thinking about following his arrest for felony murder, tampering with physical evidence, and making false statements in connection with his wife's death.

The man told police he called 911 after a "stocky, obese" man with a deep voice like Vin Diesel's, who was dressed in camouflage clothing and wearing a mask, broke into their Connecticut home and demanded money. He told investigators that the intruder shot his wife and tied him up to a chair with zip ties before fleeing the house. In an affidavit in support of an arrest warrant, the police reported they used data from the home's "alarm system, computers, cellphones, social media postings and the wife's Fitbit to create a timeline that contradicted the husband's statements to police." According to the affidavit, the husband initially said his wife had just returned home from the gym when the invader shot her. According to the arrest warrant, the fitness tracker recorded the wife walking around the house, and that it registered she walked over 1,200 feet inside the home for almost an hour after the time the husband told investigators his wife was shot. According to the arrest warrant, the panic alarm for the home's security system went off six minutes after the wife's Fitbit showed her idle. The panic alarm was activated from the husband's key fob.[12]

A similar request for data occurred in Arkansas when a prosecutor requested Amazon to produce Amazon Echo data that might be relevant to an underlying murder investigation. Amazon refused the request as overbroad, but the possible battle between Amazon and the prosecutor was rendered moot when the defendant voluntarily agreed that Amazon could release the data. The underlying incident involved a murder victim found dead in a hot tub at the defendant's home. The prosecutor hoped that the voice-activated feature of the Amazon Echo device, which answers users' questions, plays music, reads the news, and connects to other smart devices, would provide information on the death. Law enforcement authorities also were reviewing another smart device in the home—a water heater—to study the amount of water used in the early-morning hours at the home.[13]

Conclusion

In most examples listed above, one can easily list possible civil or criminal proceedings in which data from an Internet-connected device might be helpful. As society progresses further into the wonderful world of Internet-connected things, data stored on such devices will find their way into a courtroom as evidence in a civil or criminal case—a benefit for some and a curse for others. ■

Endnotes

1. Herbert B. Dixon, *Is Your Internet Device Spying on You?*, 56 Judges' J., no. 2, Spring 2017.

2. Herbert B. Dixon, *#AI, #VR, and #IoT Are Coming to a Courthouse Near You!*, 55 Judges' J., no. 4, Fall 2016.

3. Rob Price, *The Maker of an Internet-Connected Garage Door Disabled a Customer's Device over a Bad Review*, Bus. Insider (Apr. 5, 2017), http://www.businessinsider.com/iot-garage-door-opener-garadget-kills-customers-device-bad-amazon-review-2017-4.

4. Alex Hern, *Car Hacking Is the Future—and Sooner or Later You'll Be Hit*, The Guardian (Aug. 38, 2016), https://www.theguardian.com/technology/2016/aug/28/car-hacking-future-self-driving-security.

5. Kim Zetter, *Medical Devices That Are Vulnerable to Life-Threatening Hacks*, Wired.com (Nov. 24, 2015), https://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks.

6. Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, Wash. Post (Oct. 21, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/?utm_term=.d30f3d8f1762.

7. *Id.*

8. Lily Hay Newman, *Medical Devices Are the Next Security Nightmare*, Wired.com (Mar. 2, 2017), https://www.wired.com/2017/03/medical-devices-next-security-nightmare.

9. Thomas Fox-Brewster, *It's Depressingly Easy to Spy on Vulnerable Baby Monitors Using Just a Browser*, Forbes (Sept. 2, 2015), https://www.forbes.com/sites/thomasbrewster/2015/09/02/baby-surveillance-with-a-browser/#15d640aa1aa0.

10. Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage*, Wired.com (Oct. 21, 2016), https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn.

11. Maria Korolov, *DDoS Attack on BBC May Have Been Biggest in History*, CSOOnline.com (Jan. 8, 2016), http://www.csoonline.com/article/3020292/cyber-attacks-espionage/ddos-attack-on-bbc-may-have-been-biggest-in-history.html.

12. Mary Ann Georgantopoulos, *A Fitbit Helped Police Arrest a Man for His Wife's Murder*, BuzzFeed News (Apr. 25, 2017), https://www.buzzfeed.com/maryanngeorgantopoulos/fitbit-murder?bftw=undefined&utm_term=.xvRPnN2WNR#.au2V136b3x.

13. Eliott C. McLaughlin, *Suspect OKs Amazon to Hand over Echo Recordings in Murder Case*, CNN (Apr. 26, 2017), http://www.cnn.com/2017/03/07/tech/amazon-echo-alexa-bentonville-arkansas-murder-case.