The Internet of Things (IoT) May Prove To Be "The Next Big Thing" for Lawyers

by Samuel L. Felker, CIPP/US

> When people talk about "the next big thing," they're never thinking big enough. It's not a lack of imagination; it's a lack of observation. I've maintained that the future is always within sight, and you don't need to imagine what's already there. Case in point: The buzz surrounding the Internet of Things. --Daniel Burrus for WIRED.

It seems that everything with an on/off switch is now connected to the Internet or soon will be: our cars, door locks, fitness devices, security monitors, appliances, computers, phones, lights, cameras, etc. With a simple voice command, we can now dim the house lights, adjust the thermostat, turn on security alarms, activate cameras, and shut down the house for the night. Or, even more Jetson-esque, soon we can purchase our favorite pair of sneakers and have them delivered by a drone to our front lawn within a matter of minutes. The Internet of Things (IoT)--the concept of connecting devices to the Internet and to each other--has quickly taken over our homes, our businesses and our lives. But with these technological "advances" come increasing risks--and often they are unexpected. This article will discuss the brave new world of IoT across several product lines--home devices, automobiles and medical devices--and explore what the future may hold as lawyers advise their clients about cyber security threats, privacy issues and other risks presented by IoT.

The Wired Home

Internet-connected devices, ranging from thermostats to remotely controlled security cameras and locks, promise to take our homes to an unprecedented level of comfort and convenience, but this new digital format for the home brings considerable risk. Gadgets designed for our home can talk with each other, yet they risk being overheard when communicating sensitive data. They can also be accessed controlled by malicious hackers in ways that compromise personal safety. For example, there are shocking reports of hackers gaining access to Internet-connected baby monitors which permitted the cyber-intruders to observe the infants in their nurseries. That is but one example of a potential cyber-attack that sends chills up the spine of any parent.

The FBI recently issued a public service announcement [https://www.ic3.gov/media/2015/150910.aspx] explaining some of the key IoT risks for homes, including:

- An exploitation of the Universal Plug and Play protocol (UPnP) to gain access to many IoT devices. The UPnP describes the process when a device remotely connects and communicates on a network automatically without authentication. UPnP is designed to self-configure when attached to an IP address, making it vulnerable to exploitation. Cyber actors can change the configuration, and run commands on the devices, potentially enabling the devices to harvest sensitive information or conduct attacks against homes and businesses, or engage in digital eavesdropping;

- An exploitation of default passwords to send malicious and spam e-mails, or steal personally identifiable or credit card information;

- Compromising the IoT device in a variety of ways to cause physical harm;
- Overloading the devices to render the device inoperable; and
- Interfering with business transactions by home network hacking.

As a result of these substantial risks to homeowners, the FBI recommends either securing the devices and networks with appropriate password protections, or stay away from them altogether. And, businesses that employ IoT for security or in operations are subject to the same risks.

Given these potential hazards, device manufacturers and sellers are potentially liable under traditional negligence and products liability theories, as discussed below. Imagine a security camera or locking system gets hacked, permitting theft or personal injury to the inhabitants or the business. Plaintiffs' lawyers then file suit against the device manufacturer or installer for their failure to provide reasonable cyber-security for users, or they file a class action on behalf of all purchasers of the device. Although we are not aware of current litigation like this, plaintiff's firms are advertising for individuals who have been injured or suffered data loss from IoT home devices. Litigation can't be far away.

Automobiles

Volvo, the most aggressive car manufacturer when it comes autonomous vehicles, predicts that by the year 2020 it will completely eliminate crash-related deaths in its cars. Now, it seems everyone is in the game, with Uber pushing forward with development of its self-driving Ford Fusions and GM announcing it will roll out a fleet of autonomous cars with Lyft. About the time we got used to the idea of a self-driving car, the wheels came off, literally. In May last year, a self-driving Tesla-S failed to recognize the side of a white tractor-trailer truck against a pale sky, resulting in a crash that killed a 40-year old technology consultant and autonomous vehicle enthusiast. Then reports surfaced that Uber's prototype testing got off to a bumpy start with a self-driving car turning down a one-way street before its operator took over and turned the car around.

Some suggest it's time to pump the brakes, but that does not appear to be the plan because the data looks so promising. According to the National Highway Traffic Safety Administration, every day in the United States, approximately 90 people die and 6,400 are injured in automobile accidents. It is no surprise that 94 percent of all those accidents are caused by human error. In 2013, the Eno Center for Transportation forecasted that even at just a conservative 10-percent penetration rate, autonomous vehicles would help save more than 1,000 lives per year and result in comprehensive cost savings for society of almost $18 billion annually. But if we achieved 90 percent adoption, the group estimates almost 22,000 lives would be saved yearly, and society would garner a staggering $350 billion in cost savings.

Accidents involving autonomous cars will generate a whole new set of liability theories when the fleets actually hit the road. It stands to reason that manufacturers will be assigned more liability, relative to drivers, than is currently the case with conventional cars. With no driver at the wheel, plaintiff's lawyers will no doubt focus on the manufacturers of the complex software and the automobile itself. With the ever present possibility of computer equipment failure, the car and component manufacturers will be subject to suit on theories of defective manufacture or design, including failure to warn. This shift in liability will, no doubt, dramatically change car liability insurance, since driver fault will not be the factor it is today.

Then there is the hacking problem. In 2015, Wired reporter Andy Greenberg introduced the world to a terrifying new kind of threat: that hackers could, given the right circumstances, remotely take control of a car. Specifically, his 2014 Jeep Cherokee—and possibly all kinds of newer Chryslers, which makes the Jeep. The problem with the IoT, of course, is that anything that connects to the internet has an access point, and it's in the nature of any hacker—whether they're a security researcher or a criminal—to try to exploit it. Greenberg's Jeep, for example, was hacked by two enterprising researchers who figured out that the model had vulnerabilities in its Internet-connected dashboard computer, giving them the ability to control the air conditioning and radio, to kill the engine, and to control the steering when it was in reverse. Other reports of "white hat" hacking of cars have recently surfaced but to date the U.S. Department of Transportation National Highway Traffic Safety Administration reports that no car is known to have been maliciously hacked in the wild—only by the good guys.

Nevertheless, you can imagine the liability theories that will be asserted against car manufacturers for failing to provide adequate cyber-security for the numerous systems on their automobiles. Again, it appears the car manufacturers will bear a heavier burden than ever before, since the manufacturer is ultimately responsible for the safety of the vehicle it sells. Stay tuned, because with driver fault out of the equation, or at least reduced, the manufacturer will be the target and will be expected to defend allegations that a hackable car is defective and unreasonably dangerous.

Medical Devices

In a 2012 episode of the television show *Homeland* the vice-president of the United States was assassinated when his pacemaker was hacked. Then in 2013, then Vice-President Dick Chaney announced the wireless features of his defibrillator had been disabled due to concerns that the device could be hacked. Many scoffed in disbelief and attributed the whole issue to paranoia. Now, it has come to light that thousands of medical devices, including MRI scanners, heart devices, x-ray machines and drug infusion pumps, are vulnerable to hacking, creating privacy issues and significant health and safety risks for patients. This obviously creates liability risks for manufacturers and healthcare facilities who use the devices to treat patients. Some systems were connected to the Internet by design, others due to configuration errors, but the problem also arises because often devices are still using the default logins and passwords provided by manufacturers. That provides a field-day for hackers who have an easy way in.

The issue came to the forefront when FDA issued a safety alert regarding cyber-security in July 2015 regarding a Hospira infusion pump. [http://www.allgov.com/news/top-stories/fda-issues-its-first-ever-cybersecurity-alert?news=857125]. FDA warned of the potential for remote access of the pump by an unauthorized user which could enable tampering with the dosage, causing serious health risks to patients. The issue came to FDA's attention when a "white hat" hacker disclosed it had hacked into the device and reported vulnerabilities, including the ability to control the device and obtain information from it.

Another hacker recently reported using the search engine Shodan to find 1,000’s of unprotected systems in U.S.—with one large provider, exposing over 68,000 systems with direct attack vectors to the systems and third-party organizations associated with the provider. The hacker was able to locate the device, identify its type, and even the floor and office number where it was located. The hacker also set up and monitored a "honeypot" and documented evidence of unintentional access to those devices.

Then there is the strange ongoing dispute between heart pacemaker manufacturer St. Jude and the hedge fund Muddy Waters. Muddy Waters claimed in late August that there was a “strong possibility” that almost half of St Jude’s revenue could evaporate for two years as a result of security problems in its implantable cardiac devices that were critical for patients who suffered from various heart ailments. It claimed there were flaws in the Merlin@home monitoring device which could allow it to be attacked from up to 50 feet away and estimated there were more than 200,000 such devices in the US. St Jude has fired back repeatedly at Muddy Waters, saying it stands behind the security and safety of its devices. Then in September St. Jude filed a lawsuit in U.S. District Court in Minnesota against Muddy Waters claiming it made up the hacking allegations as part of an "insidious scheme" to manipulate St. Jude's stock price. Jt. Jude has also reportedly been the subject of a lawsuit from a patient, claiming he has been advised by his doctor not to use the device.

These recent developments raise a host of red flags and have increased awareness of vulnerabilities which manufactures and users must address to reduce liability risks and protect patient safety and privacy. What we know is that some software driven, connected medical devices may be vulnerable, exposed ones, and FDA has not stepped in to specify particular cyber safety or security controls. FDA merely warns the manufacturer that it is responsible for the cyber security of its devices. Given the current landscape, this is an area ripe for product liability litigation, including class actions from patients and consumers who may be at risk.

Traditional liability theories can be easily applied to harm caused by IoT devices

It is easy to see how the move to Internet-controlled devices is a tort lawyer's dream, and it is clear the IoT may prove to be a treasure trove for creative lawyers. If a hacker uses the vulnerabilities of a device to cause harm, the injured party could sue the manufacturer alleging the device was defective due to either insufficient security controls or a failure of the manufacturer to warn of dangers it knew of with the devices' configuration. Under a product defect theory, the plaintiff could either rely upon the consumer expectation test (the device was more dangerous than a reasonable consumer would expect due to cyber vulnerabilities) or the reasonable manufacturer test (a reasonable manufacturer would not have sold the device with knowledge of the cyber defect). Then there are traditional negligence theories--that the manufacturer failed to exercise reasonable care to protect the users of the product from foreseeable risks. Manufacturers can rely on standard defenses, including contributory negligence and adequate warnings of the cyber risks in the product literature.

In the brave new world of the IoT, both consumers and manufacturers need to take note of the substantial risks to personal safety and privacy that exist, and act accordingly. Only then will IoT provide the benefits everyone is expecting in the future. You can rest assured that lawyers stand ready if the risks presented by IoT instead result in injury to the public.

Sam Felker is a shareholder at Baker Donelson and practices in the areas of products liability litigation and cyber-security in its Nashville and Fort Lauderdale offices. Sam is currently a Co-Chair of the ABA Products Liability Committee.