The Era of the Internet of Things: Can Product Liability Laws Keep Up?

By: Leta Gorman

Leta Gorman is a Director at Betts Patterson & Mines in Portland, Oregon, where she specializes in product liability, complex commercial, and construction defect litigation. She was named one of Oregon's Top 25 Women Oregon Super Lawyers in 2013 and, since 2011, she has been recognized by Best Lawyers in America and Oregon Super Lawyers. She has an AV® Preeminent™ Attorney Peer Review Rating and is included in the Bar Register of Preeminent Women Lawyers™ (Martindale-Hubbell®).

I. The Internet of Things Era

WE ARE living in an era that some refer to as the "Internet of Things" ("IoT"), where wireless connected devices know how we work, play, shop, sleep, drive, manage our homes, and medicate. IoT is a concept that represents the network of smart devices (or "things") that are connected to the Internet and to each other and have the ability to collect and exchange data on every aspect of our lives and businesses.[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] The connected devices operate on embedded sensors that automatically measure and transfer data (*i.e.*,

[1] *Internet of Things - Privacy & Security in a Connected World*, FTC Staff Report at 1 (January 27, 2015), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-work shop-entitled-internet-things-privacy /150127iotrpt.pdf (last visited May 11, 2017) (hereinafter "FTC Staff Report").

[2] Antigone Peyton, *A Litigator's Guide to the Internet of Things*, 22 RICH. J.L. & TECH. 9 at 1 (2016), available at http://jolt.richmond.edu/2016/04/01/a-litigators-guide-to-the-internet-of-things/(last visited May 11, 2017).

environmental and activity information) over a network to data stores without human interaction.[3] These data stores interact with analytic engines to collect and provide data that can be acted upon.[4]

Among connected devices are devices that allow for the remote monitoring of babies and children; devices to help you to remember to take your medications; devices to track your activity levels; devices to help monitor an aging family member; medical devices that allow your health to be monitored by your doctor and that automatically release proper levels of medication; devices that allow you to remotely monitor your home; devices that allow you to turn off appliances or change the temperature in your home; devices that allow you to feed and water your plants and pets; and refrigerators that remind you when you are out of eggs. There are smart TVs and toys. There are devices that allow cities and governments to monitor trash pick-up, traffic flows, pollution levels, electricity usage, and the structural soundness of buildings and roads. There are devices that allow companies to monitor the repair and maintenance needs of equipment and track real time marketing trends in stores. This list of IoT devices is in no way complete, and it grows longer every day.

In 2009, the number of IoT devices surpassed the number of people,[5] yet, the development and use of connected devices is really just in its infancy. By 2020, it is estimated that there could be 50 billion connected devices.[6] By way of example, only 10% of consumer cars were connected to the Internet in 2009, but in 2020, 90% of consumer cars will be connected.[7]

---

[3] *See Embedded Intelligence - Connecting Billions of Smart Sensors into the Internet of Things*, Arm Holdings, available at https://perma.cc/3HWX-QBWW (last visited May 11, 2017); *see also* Daniel Burrus, *The Internet of Things is Far Bigger Than Anyone Realizes*, https://www.wired.com/insights/2014/11/the-internet-of-things-bigger (last visited May 11, 2017).

[4] Burrus, *supra* note 3.

[5] *See* Dave Evans, *The Internet of Things: How the Next Evolution of The Internet is Changing Everything* at 3, Cisco Internet Bus. Solutions Grp. (April 2011), available at https://perma.cc/HDF9-NM6T. These are estimates for all types of connected devices, not just consumer market devices.

[6] *Id.* 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] (April 2014), available at https://perma.cc/86RJ-786G; *see also Data Set to Grow 10-fold by 2020 as Internet of Things Takes Off*, Computerweekly.com (April 2014), 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*.

[7] *Connected Car Industry Report 2013*, Telefonica at 9 (2013), available at http://websrvc.net/2013/telefonica/Telefonica%20Digital_Connected_Car2013_Full_Report_English.pdf.

"All of these connected machines mean much more data will be generated: globally, by 2018, mobile data traffic will exceed fifteen exabytes – about 15 quintillion bytes – each month. By comparison, according to one estimate, an exabyte of storage could contain 50,000 years' worth of DVD-quality video."[8]

Certainly, IoT devices can provide many benefits to consumers – convenience, home safety, medical monitoring, and reduced energy waste are a few examples. These benefits help explain IoT's rapid growth. But, these devices create both security and privacy risks.

IoT devices can be hacked and controlled by third-parties. For example, imagine if the software system for the electronic thermostat in your home is hacked and turned off. Your home is damaged as a result of frozen pipes and/or water damage. Or, imagine if your home security system is hacked and disconnected. Your home is then vandalized and robbed.[9] Or, what if your doctor's medical monitoring equipment software is hacked? Your medical device doesn't release the medicine you need to survive. Or, what if your implanted defibrillator has been reprogrammed by an unauthorized user?

There are also privacy risks related to IoT devices. The devices collect, transmit, and store consumer data, some of which is highly personal. If they are hacked, your private personal information could be shared, sold, and used. Private conversations could be exposed. Your private life is now no longer private.

Beyond these security and privacy risks, a device may also simply malfunction. A remotely operated device might fail and cause property damage such as fire or water damage. A home security device might leave doors or windows open, allowing intrusions or burglaries. Or, a medical device may fail to provide crucial medication to a patient or information to a doctor, causing serious injury or even death.

II. Can Product Liability Law Keep Up in the IoT Era?

If an IoT device is hacked and/or malfunctions, there will be new challenges with regard to product

---

[8] *See*, *e.g.* FTC Staff Report, *supra* note 1, at 2, citing to CISCO, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2013–2018* at 3 (2014), available at http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-indexvni/white_paper_c11-520862.pdf and University of Bristol, Exabyte Informatics, available at http://www.bris.ac.uk/research/themes/exabyteinformatics.html.

[9] *See*, *e.g.*, Julie Jacobson, *Quirky 'Terribly Embarrassed' Over Wink Home Automation Hub Recall* (Updated) CE Pro (April, 20, 2015), http://www.cepro.com/article/quirky_terribly_embarrassed_over_wink_home_automation_hub_recall#.

liability law. Traditional notions of product liability law provide that a product manufacturer, component part supplier, or seller (and others who make products available to the public) are to be held liable if they put a defective product into a consumer's hands and the defect causes personal injury or property damage. A consumer can sometimes be liable for mishandling or misusing a product as well. Product liability claims are based on state laws and brought under negligence, strict liability, or breach of warranty theories.[10] With an IoT device, however, these traditional notions will be challenged. What product liability law will look like in 2020 is an unknown. Today, unfortunately, there are more questions than answers.

For example, how are damages related to privacy issues to be compensated? What if there is a security breach and private information is obtained and even shared but not used. How do you quantify those damages? Damages related to privacy issues are intangible and hard to quantify. These types of damages also create legal questions of standing.

In addition, how do you allocate responsibility for damages? Does legal fault lie with the hacker, with the manufacturer, or with the owner who may have failed to properly secure the product (*i.e.*, by using a sufficiently strong password or by timely updating the software)? If there is a software failure versus an actual defect in the product, should the maker of a product be held liable for the software failure? What if the manufacturer of the product or the software failed to include sufficient security designs? What about component part liability? Traditional product liability law holds that defective component part manufacturers can be held liable. Is software a component part?

Are there contracts between the software company and product manufacturer that allocate the risk of a potential hack and resulting damages between them? Are those contracts specific to the product and negotiated at arm's length? Was the consumer compelled to sign a standard form agreement that automatically waived claims in order to use the software that accompanied the product?

What about insurance? Will traditional insurance policies, which generally cover losses that result in property damage or bodily injury resulting from a product defect, apply when an IoT product failure occurs? Will insurers begin to redesign their policies to provide specifically designed coverage to prevent any potential gaps in coverage?

At trial, what standards can be used to suggest an IoT's alleged

[10] *See generally* RESTATEMENT (THIRD) OF TORTS: PRODUCT LIABILITY §§ 1-2 (1998).

design, manufacturing, or other flaws fell below a minimum acceptable level? There are some developing standards relating to IoT but nothing that is considered universally acceptable. For example, the Institute of Electrical and Electronics Engineers ("IEEE") has a "Standard for an Architectural Framework for the Internet of Things (IoT),"[11] the International Organization for Standardization ("IOS") and the International Electrotechnical Commission ("IEC") have a family of standards for security management systems, [12] and the International Telecommunications Unit ("ITU") has an Internet of Things Global Standards Initiative.[13] The United States Federal Trade Commission is taking a serious look at what kind of regulations are needed for personal and home devices that collect and transmit user data[14] and, at the end of 2016, the U.S. Food and Drug Administration issued final guidance regarding the need for post market management of cybersecurity in medical devices.[15] IoT is so broad and complex that no single standards organization has the possibility of being the one entity to pull it all together. How will liability be judged at trial if there is no minimum set of safety precautions or requirements?

If a product has vulnerabilities that allow it to be hacked, can a consumer allege the device was defective due to insufficient security controls or a failure of the manufacture to warn of dangers it knew of regarding the device's configuration? And, has the consumer waived any rights regarding the software pursuant to any licensing agreement that was provided with the product?

Who has custody, ownership, and control over the data collected? Does the consumer own the data even though the data is maintained by someone else? Will there be chain of custody issues with regard to the data collected?

Software in connected devices will also impact discovery and investigation in IoT cases. There will be an added layer of complexity to any investigation with regard to what happened. In addition, the

[11] IEEE Standards Association, P2413 – Standard for an Architectural Framework for the Internet of Things (IoT), available at https://standards.ieee.org/develop/project/2413.html.

[12] ISO/IEC 27000 family – Information security management systems, available at https://www.iso.org/isoiec-27001-information-security.html.

[13] ITU Internet of Things Global Standards Initiative, available at http://www.itu.int/en/ITU-T/gsi/iot/ Pages/default.aspx.

[14] *See*, *e.g.*, FTC Staff Report, *supra* note 1, at 1.

[15] *Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff*, U.S. Food & Drug Administration, December 28, 2016, available at https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf.

discovery process in IoT litigation could implicate privacy concerns. Plaintiffs may have to turn over the devices or tablets from which they operate a connected product that is the subject of the lawsuit. The devices may be helpful in determining if appropriate software updates occurred to allow the connected device to function properly or if a hack occurred. The information may help provide evidence of negligence on the part of the consumer or perhaps that of a hacker whose hack makes the product cause damage. Notwithstanding the arguable need for discovery of information on personal devices, plaintiffs may be reluctant to turn over devices that contain personal data.

Finally, even a small glitch in a network can impact hundreds or thousands or millions of products. This is a perfect formula for product liability no-injury class action litigation. Below, this article provides examples of cases that are already beginning to touch upon many of these issues.

III. IoT Device Cases

There have been cases involving IoT connected devices, but instead of litigating product liability issues, the issue of standing (lack of actual harm) is the prevalent theme in these cases.[16]

In *Cahen v. Toyota Motor Corp.*,[17] Cahen filed an over 300-page national class action against Toyota, Ford, and General Motors. Cahen alleged, among other things, that these car manufacturers equipped their vehicles with computer technology that is vulnerable to hacking. Plaintiffs alleged that a hacker can communicate remotely (through Bluetooth or cellphone) with computers controlling many of the vehicles' functions, resulting in a complete loss of driver control over steering, accelerating, and braking. Plaintiffs claimed that the manufacturers were aware of these security issues but nevertheless advertised their products as safe. As such, plaintiffs asserted that the auto companies breached, among other things, the implied warranty of merchantability and contract/ common law warranty and committed fraud.

The auto companies moved to dismiss on various grounds, including lack of standing. The defendants argued "plaintiffs do not allege any hacking incidents that have taken place outside of controlled settings, and that the entire threat rests on the

[16] "Actual or imminent" injury—not just "conjectural or hypothetical" harm— is the "irreducible minimum" of all lawsuits under the Constitution. Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992). (Scalia, J.) "No principle is more fundamental to the judiciary's proper role in our system of government." DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006) (Ginsburg, J.).

[17] 3:15-cv-01104 (N.D. Cal. March 10, 2015).

speculative premise that a sophisticated third-party cyber-criminal may one day successfully hack one of plaintiffs' vehicles." Citing traditional automobile product liability cases, the court agreed with defendants, determining that the potential risk of future hacking was not an injury in fact. Nor was the court persuaded that standing could be supplied because of a "benefit of the bargain theory," holding: "The plaintiffs have not, for example, alleged a demonstrable effect on the market for their specific vehicles based on documented recalls or declining Kelley Bluebook values."[18] The case was dismissed. Plaintiffs have appealed the dismissal to the Ninth Circuit, however.

In another suit against Chrysler Group, [19] plaintiffs alleged that a security flaw in "infotainment" centers manufactured by co-defendant Harman International Industries was installed in certain vehicles. Plaintiffs alleged the "infotainment" center is "exceedingly hackable," permits hackers to "remotely take control" of the steering, acceleration, and braking, and lacks the ability to quickly and effectively patch any software security flaws. The complaint alleges negligence, fraud, and breach of warranties.

Following defendants' motion to dismiss on, among other grounds, the speculative nature of the damages, the court dismissed certain claims and trimmed others. According to the court, plaintiffs lacked standing to seek damages for the threat of future hacking. But, the court found plaintiffs did have standing to sue for damages for the diminished value of the car because "the ongoing vulnerabilities have reduced the market value of their vehicles."[20]

Cardiac devices, such as pacemakers and defibrillators, were the subject of *Ross v. St. Jude Medical Inc*.[21] The devices at issue include an in-home monitoring system and use radio frequency wireless technology. The technology allows the implanted devices to be monitored remotely. The plaintiff filed a proposed class action alleging that the system lacked the "most basic security defenses." The plaintiff was not physically injured in any way but he claimed that the devices could be disabled or their batteries drained if they are hacked. Plaintiff voluntarily dismissed the case, without prejudice, in December 2016.

In *Baker v. ADT Corp*.,[22] plaintiff filed a class action alleging that ADT's wireless security and monitoring equipment could be

[18] Cahen v. Toyota Motor Corp., 147 F. Supp.3d 955, 971 (N.D. Cal. 2015).
[19] Flynn v. FCA US LLC, 3:15-cv-855 (S.D. Ill. Aug. 4, 2015).
[20] *Id.* at 9.
[21] No. 2:16-cv-06465 (C.D. Cal. Aug. 26, 2016).
[22] No. 2:15-cv-02038 (C.D. Ill. Nov. 9, 2014).

remotely turned on or off using technology accessible to the public. In addition, plaintiff claimed that third parties "can also hack into ADT's wireless systems and use customers' own security cameras to unknowingly spy on them."

Plaintiff in *Baker* alleged that his system was hacked at least twice by an unauthorized third party, which "caused the system to be falsely triggered, which in turn caused ADT to contact Plaintiff and have the police called to Plaintiff's home."[23] But rather than quantify any particular harm that flowed from those "false alarms," plaintiff's allegations focused instead on several of ADT's marketing statements, including that ADT's monitoring centers were "equipped with secure communication links." His suit alleged violations of the Florida and Illinois consumer fraud statutes and claims for strict product liability and unjust enrichment.

Although the claims for strict product liability and unjust enrichment were ultimately dismissed, the case continues with consumer fraud claims based on the "secure communication links" representations in ADT's advertising.

In re VTech Data Breach Litigation[24] involved a manufacturer of children's learning toys that link to certain web-based services. The complaint alleges that in November 2015, an overseas hacker illegally bypassed VTech's security measures, obtained customer data, such as profile pictures, emails, passwords and nicknames, and provided the data to a journalist. The hacker was arrested shortly thereafter.

According to the complaint, the journalist who broke the story wrote: "[VTech] left thousands of pictures of parents and kids and a year's worth of chat logs stored online in a way easily accessible to hackers." The plaintiffs alleged, among other things, an increased risk of harm and diminished value of the products. They asserted claims for breach of contract, breach of the warranty of merchantability, and violations of state consumer protection laws.

In April 2016, the defendants filed a motion to dismiss alleging that the plaintiffs suffered no actual injury, as the plaintiffs did not plead that the data traveled beyond the hacker, the journalist, and a security analyst, and, as such, that plaintiffs lacked standing. The defense argued that there can be no liability for a hacker who neither intends nor accomplishes any harm beyond pointing out the vulnerability in the toy's software system. The

[23] *Id.*

[24] No. 1:15-CV-10889 (N.D. Ill. Dec. 3, 2015).

defendants' motion to dismiss is still pending.

Another "connected" toy that resulted in litigation is "Hello Barbie."[25] Plaintiffs alleged negligence, unfair competition, and privacy violations against the doll's manufacturer, Mattel Inc., and ToyTalk Inc., which managed the toy's online technology. Plaintiffs alleged the doll was designed to engage in conversation with a child, record each conversation, and collect and store the recordings in the cloud. The complaint alleged that security issues had been discovered, including a vulnerability through which a hacker could "impersonate a doll in order to lure an unsuspecting user into connecting to and supply[ing] user information to an impersonated doll." There was no allegation of actual malicious hacking of the accounts or misuse of the information in the manner identified that caused direct harm to plaintiffs.

The defendants removed to federal court[26] and filed motions to dismiss based on standing and other grounds, and also moved to compel arbitration. The court never ruled on the motions because plaintiffs agreed to dismiss the case with prejudice.

IV. Conclusion

Given the predictions regarding the number of IoT devices expected to exist in 2020 and the amount of data traffic expected to be created, the number of consumer claims will only continue to grow. Traditional product liability theories will need to be examined and re-examined in this new era. The IoT has not only changed and will continue to change the way we live … it will change how we think about security, privacy, and traditional notions of product liability law. In time, we will learn if product liability laws can keep up.

[25] *See* Archer-Hayes v. ToyTalk, Inc., No. BC603467, 2015 WL 8304161 (Cal. Super. Dec. 7, 2015).

[26] *Id.*