CARLTON FIELDS

A Look At Manufacturer Liability For The Internet Of Things

October 04, 2016

The internet of things refers to the connection of everyday objects to the internet or other networks. Some common examples are home thermostats, smart TVs, wireless home cameras, and even refrigerators that can tell when a household is running low on milk. By some estimates, the number of connected devices in use will increase by 5.5 million devices per day to exceed 6.4 billion devices by the end of 2016.[1] For industry, the opportunity to manufacture and profit from connected products comes with complications. The typical manufacturer of such high-tech devices has long protected and secured its own internal network — that is, it has closed and locked the door to its business. But each day that same business churns out thousands of unlocked, open windows in the form of unsecured, internet-connected consumer goods that invite hackers to do harm. There is a serious risk that in racing these smart devices to market, companies will fail during the research and development phase to vet them for vulnerabilities to hacking attacks. Once on the market, these vulnerabilities may be exploited by hackers, and that could mean significant legal liability for manufacturers in the form of class actions and other litigation. This article summarizes and briefly analyzes recent litigation across several industries, and then makes some predictions and suggestions as to manufacturer liability for products that are part of the IoT. **Automobiles** Plaintiffs firms have a great deal of experience suing automakers, so it is not surprising that two of the first major lawsuits concerning the IoT are putative class actions against automakers. The largest two have come to arguably contrary results on standing, which is emerging as a major issue in these cases. The first is a putative class action against Ford Motor Co., General Motors and Toyota. In Cahen v. Toyota Motor Corp., 3:15-cv-01104 (N.D. Cal. March 10, 2015), the plaintiffs alleged, among other claims, that these manufacturers equipped their vehicles with computer technology that is vulnerable to hacking. According to the complaint, a hacker can communicate remotely (through Bluetooth or cellphone) with the small network of computers controlling many of the vehicles' functions, resulting in a complete loss of driver control over steering, accelerating, and braking. The plaintiffs claimed that the manufacturers were aware of these security vulnerabilities but nonetheless touted their products as safe. As such, plaintiffs asserted that Ford, GM and Toyota breached, among other things, the implied warranty of merchantability and contract/common law warranty as well as committed fraud. The auto companies moved to dismiss on grounds that included lack of standing. The defendants argued "that plaintiffs do not allege any hacking incidents

that have taken place outside of controlled settings, and that the entire threat rests on the speculative premise that a sophisticated third party cybercriminal may one day successfully hack one of plaintiffs' vehicles."[2] Citing traditional automobile product liability cases, the court agreed, determining that the potential risk of future hacking was not an injury in fact.[3] 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."[4] Plaintiffs have appealed the dismissal to the Ninth Circuit. The second major lawsuit is against Chrysler Group. In Flynn v. FCA US LLC., 3:15-cv-855 (S.D. Ill. Aug. 4, 2015), the plaintiffs sought damages stemming from an alleged security flaw in "infotainment" centers manufactured by co-defendant Harman International Industries and installed in certain RAM, Chrysler, Jeep and Dodge vehicles. The complaint alleges that the infotainment system is "exceedingly hackable," permits

hackers to “remotely take control” of the steering, acceleration, and braking, and lacks the ability quickly and effectively for software security flaws to be “patched.” The 17-count complaint alleges negligence, fraud, and various violations of warranties. The defendants moved to dismiss, citing among other things the speculative nature of the damages. The court on Sept. 23, 2016, dismissed certain claims and trimmed others. The court held, as in Cahen, that plaintiffs lacked standing to seek damages for risk of future hacking. But unlike Cahen, the Flynn court held that the plaintiffs had standing to sue for damages for the diminished value of the car because “the ongoing vulnerabilities have reduced the market value of their vehicles.” What might have made the difference in Flynn was a 2015 article in Wired magazine drawing attention to the vulnerability[5] — alleged to have had a real impact on resale prices — and allegations in the complaint that the recall did not fix all the vulnerabilities of the system. **Children’s Tech** Another area of early action for this type of consumer litigation is in web-connected children’s toys, likely because of the headline-grabbing impact of any hack that involves children’s privacy. Perhaps the most prominent example is a lawsuit in Illinois federal court against certain VTech entities, which manufacture children’s learning toys that link to certain web-based services.[6] According to papers in the case, in November 2015, an overseas hacker illegally bypassed VTech’s security measures, obtained customer data from the web services (including profile pictures, emails, passwords and nicknames), and provided the data to a technology journalist. The hacker was arrested shortly thereafter. The technology journalist who broke the story was quoted in the complaint as writing: “[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 claims, breach of contract, breach of the warranty of merchantability, and violations of state consumer protection law. Similar to the plaintiffs in the automobile cases, the plaintiffs alleged an increased risk of harm and that the value of the products had diminished. In April 2016, the defendants filed a motion to dismiss alleging that the plaintiffs had suffered no actual injury, as the plaintiff 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 argument was that there was no allegation the hacker intended or accomplished any harm beyond pointing out the vulnerability. The defendants’ motion to dismiss is pending. Another connected toy that led to litigation is “Hello Barbie.” In that case, according to the complaint first filed in Superior Court in Los Angeles, the doll was designed to engage in conversation with a child, record each conversation, and collect and store the recordings in the cloud.[7] 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.” Similar to the above automobile cases, there was no allegation of actual malicious hacking of the accounts or misuse of the goods in the manner identified that caused direct harm to plaintiffs. Nonetheless, plaintiffs alleged negligence, unfair competition and privacy violations against the doll’s manufacturer Mattel Inc., and ToyTalk Inc., which managed the companion online application. The defendants removed to federal court, and filed motions to dismiss based on standing and other grounds, and also moved to compel arbitration.[8] The court never ruled on the motions because plaintiffs agreed to dismiss the case with prejudice. **Medical Devices** Connected pacemakers and

other cardiac devices are another area where plaintiffs are testing the waters of mass actions. In Ross v. St. Jude Medical Inc., No. 2:16-cv-06465 (C.D. Cal. Aug. 26, 2016), the products being challenged are a variety of St. Jude Medical's implants — including pacemakers, defibrillators and heart resynchronizers — that use radiofrequency wireless technology. This feature allows the implanted devices to be monitored remotely with in-home equipment, reducing visits to the doctor's office. In this putative class action, the plaintiff cites a "report" alleging that these cardiac devices and the in-home transmitter used to connect to them allegedly lacked even the "most basic security defenses." The plaintiff claims that the devices are exposed to potential attacks in which hackers could disable the device or drain its battery. St. Jude is vigorously contesting the allegations and has even filed a separate defamation action against the issuers of the report that led to the putative class action. Meanwhile, the plaintiff in the product liability case alleges breach of express warranty, fraudulent concealment, negligence, and unjust enrichment. While this products case is in its infancy, it will be important to monitor, given the ubiquity of these medical devices and the potential legal exposure if the claims proceed. **Home Security Systems** The last place one might expect to find network security risks are within a home security system, yet that is exactly what is alleged in Baker v. ADT Corp., No. 2:15-cv-02038 (C.D. Ill. Nov. 9, 2014). The plaintiff filed this class action alleging that ADT's wireless security and monitoring equipment — which ADT advertised as secure and reliable — could be remotely turned on or off using technology readily available 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." The plaintiff 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." But rather than quantify any particular harm that flowed from those "false alarms," the 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. The defendants' motion to dismiss turned not on standing but, in part, on the legal sufficiency of claims based on marketing statements, including arguing that many of the statements as to security were "puffery." In October 2015, the court granted the motion to dismiss in part, dismissing the strict liability count, but leaving unjust enrichment. The court kept only those portions of the consumer fraud counts based on the "secure communication links" language in the advertising. This case continues to progress through discovery. **The Future of IoT Liability** Initial standing problems have stalled many of the early cases that are testing manufacturer liability when it comes to the IoT. This is a function of "gray hat" hackers, working with or without journalists and plaintiffs, who identify the vulnerabilities without doing any additional harm with the data collected. In many ways, the centrality of standing tracks some of the first consumer data breach cases, in which plaintiffs fought to prove actual injury based only on a risk that their compromised data would be used to commit identity theft and other fraud but could show no tangible loss. But the potential for real harm from the IoT's vulnerabilities makes the modern, personal-information-only data breach cases — presenting only a harm that in many instances can be ameliorated with identity theft restoration services — look less

significant. After all, in an IoT case, allegations of the failure of life-prolonging medical implants, the vulnerability of automobile steering systems, and the privacy of residential security cameras, will no doubt scare judges and juries alike. That could mean huge damage awards against manufacturers and anyone else in their supply chain if these cases reach trial. Companies should integrate into product design for internet-enabled consumer goods both the appropriate systems security and the appropriate legal security, including as necessary waivers, "clickwrap," and other assumptions-of-the-risk mechanisms that are now standard practice in the sale of software. For software-supported items, like connected automobiles, much of what had been accomplished through recalls can now be accomplished through remote patching, just like the updating of a desktop computer's security software. Companies should also consider liability-shifting provisions in their agreements with vendors that administer or manufacture the "connected" portion of their Internet-connected products. Lastly, traditional cost shifting in the form of appropriate insurance coverage should be a part of any company's management of IoT liability. The bottom line is that, while the IoT poses great opportunities for manufacturers, its risks should not be overlooked in the race to get the next big product to market.

The authors thank Tampa associate Colton Peterson for his research in support of this article. -- [1] Rob Van der Meulen, Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015, Gartner.com (Nov. 10, 2015), http://www.gartner.com/newsroom/id/3165317.
[2] Cahen v. Toyota, 147 F. Supp. 3d 955, 966 (N.D. Cal. 2015).
[3] Id. at 966-69, 974.
[4] Id. at 970-71.
[5] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway – With Me in It," Wired (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[6] In re: VTech Data Breach Litigation, No. 1:15-CV-10889 (N.D. Ill. Dec. 3, 2015).
[7] Archer-Hayes v. ToyTalk, Inc., No. BC603467, 2015 WL 8304161 (Cal. Super. Dec. 7, 2015).
[8] Archer-Hayes v. ToyTalk, Inc., No. 2:16-cv-02111 (C.D. Cal.).

Authored By

John E. Clabby

Related Practices

Cybersecurity and Privacy
Health Care
Pharmaceuticals and Medical Devices
Technology
Telecommunications

Related Industries

Health Care
Technology
Telecommunications