Smart Defenses For Smart Devices: Strategies for Defending Product Liability Claims Arising From Internet of Things Technology

David J. Oberly

Background

The "Internet of Things" (IoT) generally refers to the network of physical devices (or "things") that are connected to the Internet, collecting and sharing data. The IoT has digitalized the physical world and has transformed common, everyday objects into smart devices that connect everything from watches to refrigerators to the Internet. In the process, the IoT revolution has brought with it previously-unimaginable benefits in the form of efficiency, convenience, safety, and savings, just to name a few. Many have called the rise of the IoT the third major technological revolution, behind the Industrial Revolution and the creation of the Internet. Today, there are a wide range of applications and devices that we use in our daily lives that are impacted by the IoT. With that said, at the present time we are just in the early stages of the IoT movement. In fact, some experts estimate that by 2020, the IoT will be comprised of somewhere between 20 and 50 *billion* connected devices.

The range of different smart devices on the market today and their associated risks raise substantial issues regarding the application of traditional product liability law to these new technologies. Importantly, many of these issues may serve as significant roadblocks to plaintiffs who seek to establish actionable product liability claims as a result of malfunctions or hacking incidents related to IoT technology, all of which can be utilized by defense counsel to defend against and defeat IoT product liability litigation.

Negligence Claims

First, several challenges arise in connection with a plaintiff's ability to pursue a negligence-based design or manufacturing defect claims, as the collective, collaborative process of developing team-designed software poses significant problems as it relates to establishing a commonly accepted duty of care. At the present time, the Federal Trade Commission ("FTC") is currently in the process of analyzing this issue. The FTC has filed suit against over 50 companies, alleging that these entities did not provide sufficient security to protect consumers who use their products and services. While none of these lawsuits have been resolved to date, this litigation may very well shape the standard of care for IoT devices in future litigation.

Furthermore, plaintiffs will also likely face significant challenges in connection with pursuing negligence-based failure to warn claims as well. Generally, manufacturers owe a duty to warn consumers of the reasonably foreseeable dangers created by the use of their products. Because IoT products are comprised of internet-connected devices, manufacturers have a duty to warn of the traditional dangers and hazards that may result from the use of their devices. Importantly, however, IoT technologies also carry with them a risk that third parties could access IoT devices and improperly obtain data, cause property damage, or even bring about personal injury. Here, because of the intervening cause of damage stemming from breaches of vulnerable IoT device software—that of a criminal or tortious act committed by a third party—liability may

be significantly limited for hacking incidents involving smart devices, as significant questions exist as to whether a manufacturer's duty extends to warn of the risk of breach by third-party hackers. To date, courts have not addressed whether the duty of care on the part of manufacturers extends to third-party data breaches. However, even if a risk of this nature is foreseeable, it entails the criminal actions of third-party hackers. Importantly, as a general rule most courts have concluded that a defendant has no duty of care to protect others from third-party criminal actions. Furthermore, while courts are split on whether companies owe a duty of care to safeguard third-party data that is in the actual possession of the company—for example, data stored on a computer's IoT device—many courts have concluded that no such duty exists. As such, plaintiffs may face an uphill battle in establishing failure to warn claims in connection with the unauthorized access of their personal data stemming from an IoT device data breach.

Strict Liability Claims

In the alternative, a plaintiff could choose to pursue a strict product liability claim. Strict product liability does not involve any principles of duty or foreseeability. The fact that a product is released to customers, and a defect in the product caused injury—standing alone—is sufficient to hold a product manufacturer, supplier, distributor, or retailer liable for the damage caused.

One major challenge for plaintiffs relating to strict liability claims pertains to what test to apply to IoT-focused litigation. Given the nature of software vulnerabilities, it is likely that most insecure IoT device product liability claims would be evaluated as design defect claims. Generally, product liability law provides two differing tests to determine whether a design is defective. The first test pertains to the "risk-utility" test, which analyzes whether the foreseeable risks of harm posed by the product could have been lessened or avoided by the adoption of a reasonable or alternative design. The second test is known as the "consumer expectations" test, which asks whether the product "failed to perform as safely as an ordinary consumer would expect when used in an intended or foreseeable manner." Courts are largely split across jurisdictions over the question of what standard to apply in design defect claims. Of the two, the consumer expectations test is likely to be the more difficult to implement to insecure software defect claims, as the test is poorly suited to address defects in complex systems. Moreover, in the event this test is applied, plaintiffs may face an uphill battle in demonstrating a defect, as defense counsel could persuasively argue that due to the pervasiveness of hacking events today, consumers should expect that hackers may be able to infiltrate their software.

Breach of Warranty Claims/End-User Licensing Agreements

Moreover, plaintiffs will also likely face significant hurdles in connection with pursuing product liability claims under the final potential avenue for compensation, which pertains to breach of warranty claims. In particular, plaintiffs will likely run up against significant roadblocks in maintaining actionable breach of warranty claims due to the stringent end-user licensing agreements that accompany nearly every smart device. In this regard, almost all IoT devices employ restrictive end-user licensing agreements which disclaim any and all liabilities stemming from software failures of their products. As such, the ability to assert a breach of warranty product liability action will be foreclosed in almost all cases.

Standing

Finally, Article III standing represents another significant issue that will undoubtedly arise in the context of IoT product liability claims. To demonstrate Article III standing in federal court, a plaintiff must satisfy a three-part test, and is required to show an: (1) injury-in-fact; (2) sufficient causal connection between the injury and the conduct complained of; and (3) a likelihood that the injury will be redressed by a favorable decision. Most importantly, a plaintiff must establish the injury-in-fact element of standing by showing an injury that is concrete and particularized and actual or imminent, not conjectural or hypothetical.

With respect to IoT devices, courts considering product liability claims have traditionally rejected plaintiffs' claims that the access or dissemination of their personally identifiable information (PII) "diminished the value" of their PII. With that said, an actual data breach of a smart device resulting in the theft of the user's PII may potentially constitute a sufficient injury to confer standing based on the "substantial risk of harm" resulting from the breach, although the courts are split on this issue at the present time. Of note, the Seventh Circuit Court of Appeals in *Remijas v. Neiman Marcus Grp., LLC,* 794 F.3d 688 (7th Cir. 2015), has held that plaintiffs have standing based on the "substantial risk of harm" resulting from a data breach of personal payment information, and their lost time and money expended in mitigating against future identity theft. Likewise, in *Galaria v. Nationwide Mutual Insurance Company,* No. 15-3386 (6th Cir. Sept. 12, 2016), the Sixth Circuit held that allegations of a substantial risk of harm resulting from hackers' targeted theft of personal identifying information, coupled with reasonably incurred mitigation costs, is adequate to demonstrate a sufficient injury-in-fact to confer Article III standing.

Conversely, in *Beck v. McDonald*, 848 F.3d 262 (4th Cir. Feb. 6, 2017), the Fourth Circuit held that the risk of future identity theft stemming from a data breach, without more, is inadequate to demonstrate a sufficient injury-in-fact to confer Article III standing. Similarly, in in *Alleruzzo v. SuperValu, Inc.,* No. 16-2378 (8th Cir. Aug. 30, 2017), held that an increased threat of future identity theft faced by victims of a data breach stemming from the theft of credit card information by malicious hackers was insufficient to create a cognizable injury-in-fact for purposes of Article III standing. Thus, where an IoT device is hacked and the user's personal information stolen, the user of the device may be precluded from establishing an actionable product liability claim stemming from the data breach due to the Article III standing hurdle.

The Final Word

The IoT has not only changed how we go about our day-to-day lives, but will also have a significant impact on the nature and nuances of product liability litigation as well. Given the widespread forecasts regarding the expected expansion of the IoT universe in the near future, the number of product liability claims filed in connection with smart devices will continue to increase in number as time progresses. While traditional product liability principles will generally apply to IoT defect and hacking claims, plaintiffs will face a number of challenges and obstacles to overcome in order to establish an actionable product liability claim in connection with the use of smart technology. As such, product liability defense litigators should ensure that they stay abreast to this rapidly evolving area of law, which the courts will continue to develop and refine as IoT technology becomes even more prevalent in our everyday lives. At the same time, product liability

attorneys are well advised to add the defenses discussed above to their litigation tool belts, and should seek to deploy these robust defenses to liability and damages whenever possible.