Journal of International Technology and Information Management

Volume 31 | Issue 1 Article 3

2022

Will Products Liability Litigation Help Protect IoT Users from Cyber-Physical Attacks?

J Royce Fichtner
Drake University, royce.fichtner@drake.edu

Troy J. Strader
Drake University, Troy.Strader@drake.edu

Will Products Liability Litigation Help Protect IoT Users from Cyber-Physical Attacks?

Cover Page Footnote

The authors would like to thank Austin Decker for his research assistance on this project.

Will Products Liability Litigation Help Protect IoT Users from Cyber-Physical Attacks?

J Royce Fichtner
(*Drake University*)

Troy J. Strader
(*Drake University*)

ABSTRACT

While there is an identifiable trend towards protecting consumers from data breaches and data misuses related to IoT devices through new legislation, new regulations, government enforcement actions, and private lawsuits, there has been little progress towards creating similar legally enforceable standards of care for "cyber-physical device security." This article explores this underdeveloped area of academic inquiry into cyber-physical device security within the context of product liability litigation in the United States. The two questions addressed in this article are: (1) Have there been any successful products liability court decisions in the United States that have held IoT manufacturers liable for creating IoT products with inadequate cyber-physical device security; and (2) Is it likely that product liability litigation will soon lead to significant change in IoT cyber-physical device security? Analysis of laws, regulations, and court cases shows that the answer to both questions is negative. These findings have implications for IoT device users, device manufacturers, and the government agencies whose job it is to deter data breaches and other IoT-related cyberattacks.

Keywords: Internet of Things (IoT), Product liability law, Cyber-physical device security, Information technology law

ISSN: 1941-6679-On-line Copy

INTRODUCTION

In the past fifty years there has been a dramatic increase in the number of devices connected to the Internet, but there has also been an equally large increase in opportunities for data breaches and other cyberattacks. In the early days of the Internet, a small number of mainframe computers were connected, but today the Internet connects all forms of computers and smart phones as well as home, car, and wearable devices. As Internet capacity has expanded due to improvements in computer processing power and network bandwidth, new applications have been created that have motivated users to connect to this global information system. In the 1970s and 1980s the Internet was primarily used for electronic file sharing and e-mail by a small number of users at educational institutions and government agencies. There was little incentive for cyberattacks because the system was not easily accessible and the value of the data that could be stolen was limited. This all changed in the early 1990s when the Internet was opened for commercial activity. Massive numbers of individual users, small and large businesses, and other global organizations connected to the Internet because it enabled easy worldwide communication and the development of a global marketplace. New cybercrimes arose that took advantage of this increased usage because it enabled large-scale data breaches and electronic theft of financial assets and intellectual property. Laws to protect users were slow to develop because legislators did not understand the technical capabilities and security issues associated with these new and rapidly changing Internet applications.

More recently, the Internet of Things (IoT) has further expanded Internet use because it enables a variety of connected devices to both collect and analyze data, as well as to physically interact with the real world. These IoT devices allow for new and innovative Internet applications for consumer products, so potential cybercrimes now go far beyond the initial computer-centric possibilities. As noted by Abomhara and Køien (2015), connected devices or machines are extremely valuable to cyber-attackers, who now have a pathway to infiltrate and impact a person's car, house, or embedded medical device. Because many IoT devices collect valuable data about the user through sensors, microphones, speech recognition technology, and Global Positioning, there are grave concerns about the potential theft of that data by hackers or the unauthorized use of that data by the IoT device manufacturer.

But many IoT devices present concerns beyond misuse of data because they can interact with the real world through actuators that compel physical movement, such as unlocking doors remotely, turning off a car's engine, or stimulating a heart back

ISSN: 1941-6679-On-line Copy

.

into rhythm. If an unauthorized person is able to circumvent weak security measures and gain functional control of the device, this could result in significant property damage or bodily harm. For example, a malicious hacker could turn off the furnace in a home, open a garage door, shut down an insulin pump, overtake a car's transmission system, or overheat a coffee-maker. When one considers that there will be an estimated 30.9 billion IoT devices by 2025 (Vailshery, 2021), and that IoT devices are vulnerable to many different layers of potential cyber-attacks (Alaba et. al., 2017; Valente et. al., 2019), the potential for harm from these IoT devices is alarming.

To date, the bulk of the public's attention has centered on the theft or misuse of IoT collected data. U.S. lawmakers have begun to react by creating deterrents that impose liabilities on IoT manufacturers for inadequate data security or unauthorized use of collected data through statutes such as the California Consumer Privacy Act, the California Privacy Rights Act, the Illinois Biometric Information Act, and the New York Stop Hacks and Improve Electronic Data Security Act. Federal regulators have also taken notice and used their enforcement powers to hold IoT manufacturers responsible for inadequate data security and improper use of the data collected by such devices. For example, the Federal Trade Commission (FTC) has brought hundreds of enforcement actions against companies whose data protection practices contradict their posted data protection policies. (Mulligan et al., 2019).

While there is an identifiable trend towards protecting consumers from data breaches and data misuses related to IoT devices through new legislation, new regulations, government enforcement actions, and private lawsuits, there has been little progress towards creating similar legally enforceable standards of care for "cyber-physical device security," what this article will define as security focused on preventing non-data related breaches that allow a hacker to physically control an IoT consumer device. Attempts to pass meaningful legislation to ensure cyber-physical device security has proven unsuccessful. For example, the Security and Privacy in Your Car Act, which, would have directed the National Highway Traffic Safety Administration and the FTC to establish new federal standards to help promote security and privacy in IoT connected automobiles as well as institute a rating system to help inform consumers how well the vehicle protects the consumer from a potential attempt to control and hack the vehicle, failed to garner enough support to become law. To date, there is no legally established minimum basic security measures, standards, or features for IoT consumer products in the United States.

There are also no statutory private causes of action related to inadequate cyber-physical device security which would automatically enable the injured consumer to

ISSN: 1941-6679-On-line Copy

.

collect damages against the manufacturer of the insecure IoT device. Because the primary threat of IoT manufacturer liability currently centers on inadequate protection of data or misuse of data, there is simply less incentive to invest in adequate cybersecurity when a device does not collect data.

This disjointed growth of new laws to protect consumers from the various dangers of IoT devices mirrors the uneven growth of academic inquiry in this area. Nash notes that the main questions relating to IoT devices within the academic legal environment have primarily focused on issues relating to data protection and consumer privacy (Nash, 2021). A common finding from academic studies is that the current legal framework does not adequately protect IoT user privacy and they recognize that new legislative approaches may be needed (Maras, 2015; Weber, 2015; Li & Palanisamy, 2018). Less attention has been given to the legal implications on the compromise and physical manipulation of the IoT device by a third party. This scenario presents several questions that need to be addressed to increase our understanding of the relationship between new Internet-enabled applications and the laws that protect private users. This article will explore this underdeveloped area of academic inquiry into cyber-physical device security within the context of products liability litigation, which is the primary legal theory whereby private individuals can hold manufacturers liable for producing defective products that cause personal injury or property damage. The two questions addressed in this article are: (1) Have there been any successful products liability court decisions in the United States that have held IoT manufacturers liable for creating IoT products with inadequate cyber-physical device security; and (2) Is it likely that products liability litigation will soon lead to significant change in IoT cyber-physical device security?

In the following sections we review the literature discussing how products liability litigation can reduce product-related injuries. We then discuss how initial attempts to use products liability litigation in the context of IoT cyber-physical device security have failed and discuss why it is unlikely that any significant progress will soon be made in this area. The article concludes with a summary of findings and implications for users, device manufacturers, and legislators.

ISSN: 1941-6679-On-line Copy

.

THE ROLE OF PRODUCTS LIABILITY IN PRODUCT SAFETY, A LITERATURE REVIEW

Many products contain inherent risks to their users. For example, automobiles are designed to propel a person at high rates of speed down streets that are littered with potential hazards. If the vehicle collides with an object or encounters a slick surface, its' occupants are put at risk. Automobile manufacturers could eliminate most risks by encasing the passenger cabin in thick lead and including other elaborate safety features designed to protect against all possible dangers. However, as economist W. Kip Viscusi notes, it does not make economic sense to ensure that all products are completely risk-free (Viscusi, 2012). The cost of producing such a vehicle would place it out of the reach of most consumers and the energy needed to propel the vehicle would have a profound negative impact on the environment.

At some point, there must be a balance between safety and efficiency. Naturally, manufacturers have the largest role in seeking this balance by designing and manufacturing products in a cost-efficient manner that, although not entirely risk free, makes them safe enough for consumers. But merely relying on manufacturers to achieve the appropriate balance is insufficient. Vernick and colleagues note that there are four other general strategies to prevent product-related injuries—legislation/regulation, education, changes to the physical environment surrounding the product, and products liability litigation (Vernick et al., 2004). Legislation and regulation can require manufacturers to implement specific safety measures. For example, the government can mandate that all vehicles contain seat belts. Education can warn users of the risks of potential harm and inform users how to modify behavior to minimize the likelihood of injury. For example, the media can educate the public on the importance of wearing seat belts. The physical environment can be altered through governmental spending, such as adding guard-rails to the roadway, to help reduce some of the potential damage associated with the risky product. Finally, private individuals can instigate products liability lawsuits to hold manufacturers accountable for selling dangerous products.

Products liability is the broad umbrella term used to identify the handful of legal causes of action that assign liability to the manufacturer, seller, or supplier of products that injure consumers (Prosser et al., 1988). The most popular cause of action is strict products liability in tort, though plaintiffs also often include claims for negligence and breach of warranty. Undoubtedly, the primary purpose of all products liability litigation is to compensate the injured consumer. But researchers have noted that products liability lawsuits play important roles that go beyond merely compensating the injured plaintiff.

ISSN: 1941-6679-On-line Copy

.

Garber argues that deterrence is the central goal of products liability. For example, the mere threat of litigation motivates manufacturers to invest in product safety and injury prevention (Garber, 1998). Products liability litigation has caused significant changes in the way manufacturers do business and the way consumer products are marketed. Many manufacturers have redesigned products, instituted programs improving quality control, and changed labeling specifically to reduce potential liability (Eads & Reuter, 1983). Likewise, the potential negative publicity of litigation incentivizes manufacturers to "weigh the potentially small cost of mitigating the defective design or manufacturing element in their product against releasing the product with defects and having to cover potentially large damages that these defects may cause." (Dean, 2018).

Products liability litigation also shines a light on risky products and brings their potential for further danger to the attention of the media, government regulators, and the public at large. Wagner details how litigation plays an indispensable role in lowering information-related barriers and revealing facts not normally available to regulators or the general public (Wagner, 2007). Products liability plaintiffs are able to use the discovery process to compel the release of internal company documents that can reveal hidden patterns of injury from the same or similar products. Vernick notes that seemingly rare, freak accidents are not always unforeseeable, pointing to one case where a child was severely injured when her vaporizer, that was marketed as "tip-proof," tipped over and caused burns to 30 percent of her body. Subsequent litigation revealed that the manufacturer knew that other children had previously suffered the same injury (Vernick et al., 2003). Llamas provides numerous examples where litigation revealed internal company documents displaying the manufacturers knowledge that their products were dangerous (Llamas, 2021).

If the discovery process had not revealed the true danger of some products, they might still be on the market today.

Products liability is also important because, as Rhode notes, litigation often kicks in "where politicians and government regulators have feared to tread." (Rhode, 2004). If legislators and regulators are slow to identify and react to risky products or unable to anticipate ways in which producers can evade regulation within the letter of the law, products liability litigation can fill the gap by holding companies liable for the dangers of the product and, in some instances, prompting legislators and regulators into action.

Thus, products liability litigation plays an important role in making products safer. If the safety of a product falls short of an efficient level, products liability litigation helps expose and publicize the danger, penalizes the producer for the shortfall, and prompts legislators and regulators to take an active interest in the product.

.

While economists such as Viscusi debate whether the uneven nature of jury awards and other shortcomings of the adversarial process make products liability litigation an economically efficient tool (Viscusi, 2012), there is no doubt that products liability litigation has played a significant role in advancing safety in some products, and in particular the automotive industry (Teret & Jacobs, 1989).

It has been noted that the security of IoT devices has been a low priority for manufacturers and that many devices lack basic security features (Johnson et. al., 2020; Noor & Hassan, 2019). One could argue that the current lack of sufficient cyber-physical device security in IoT products bears similarities to the early years of the automotive industry, where manufacturers once clearly prioritized style and performance over safety. Teret notes that a wave of products liability lawsuits in the late 1960s and 1970s changed the trajectory of automobile design and led to new safety laws and regulations that redefined what was expected from the automobile industry (Teret, 1981). Similar patterns developed in other industries. Products liability lawsuits over flammable fabrics generally increased safety in the clothing industry, high-profile litigation over medications such as Ephedra and Halcion and medical device litigation concerning products such as breast implants and intra-urinary devices have similarly resulted in safer healthcare products. Six years ago, legal commentators predicted that this pattern would continue with IoT products because a new wave of products liability lawsuits related to cyber-physical device security was on the horizon (O'Brien, 2015). The following section analyzes whether this wave materialized and whether manufacturers have been held liable for producing products with inadequate cyber-physical device security.

LEGAL PRECEDENT FOR INADEQUATE CYBER-PHYSICAL DEVICE SECURITY?

When IoT consumer products began to flood the marketplace ten years ago, it was safe to assume that we would experience a familiar pattern. Manufacturers would experiment with exciting new IoT possibilities while legislators and government regulators would be initially hesitant to take action that might stifle innovation. But then, high-profile products liability lawsuits would start to hold IoT manufacturers liable for producing devices with weak cybersecurity and then legislators and the IoT manufacturing industry would react by prioritizing cyber physical device security.

ISSN: 1941-6679-On-line Copy

.

However, this has not been the case. Even though the U.S. Department of Homeland Security demonstrated in 2007 that a cyberattack could, in fact, cause real-world physical damage by manipulating circuit breakers (Capano, 2021), there has been very little actual litigation regarding cyber physical device security.

This study utilized a systematic review of U.S. federal court decisions, U.S. state appellate decisions, and law reviews in the Lexis Nexis Academic database (now known as Nexis Uni) using the key term "products liability" paired with either the term internet, security, or "Internet of Things." To help ensure the external validity of this study, multiple variations of these key words and multiple combinations of subsets of these words were employed and the population of reported cases and law reviews containing combinations of such terms were reviewed. This comprehensive review revealed only two cases where courts have issued decisions pertaining to products liability causes of action and IoT cyber-physical device security. As described below, both of these lawsuits were summarily dismissed before the cases were ever brought to trial. To date, there is no legal precedent that demonstrates how an IoT manufacturer could be held liable via a cause of action for products liability for producing an IoT device that is hacked and then physically controlled by a third party.

Cahen v. Toyota Motor Corporation

The first of two reported products liability lawsuits related to IoT cyber-physical device security, *Cahen v. Toyota Motor Corporation* (Casetext, 2015) was prompted by Massachusetts's Senator Ed Markey, when he published a report highlighting the automotive industry's clear lack of appropriate cybersecurity measures to protect drivers from hackers that could potentially take control of the major operations of a vehicle (Markey, 2015). The plaintiffs in this class action case were a group of vehicle owners alleging numerous theories of recovery based on the notion that the vehicles from several manufacturers were improperly equipped with computer technology that was insecure and susceptible to hacking. Notably, the vehicle owners did not allege that any of their vehicles had actually been hacked, or that they were aware of any vehicles that had been hacked. Instead, they alleged that they were injured by the risk of hacking. They claimed the hacking was an "imminent eventuality" and that the manufacturer had improperly marketed the vehicles as safe. More specifically, the plaintiffs claimed the security vulnerability meant they were at risk of serious personal injury or death, their vehicles were at risk of theft or damage, and their vehicles were worth less than what they paid for them due to the hacking vulnerabilities. Early in the case, the defendants made a motion to dismiss arguing that the plaintiffs did not have standing to purse this lawsuit because of a lack of actual or impending injury.

.

"Standing" is a constitutional requirement that assures that court's only address issues where a party has suffered an actual injury to person or property or where such an injury is "certainly impending" if a particular wrong is not redressed (Casetext, 2013). If a plaintiff cannot prove an injury, the court has no jurisdiction to decide the case.

The district court granted the motion to dismiss for lack of standing, holding that the threat of injury was merely speculative because it was based on the premise that a sophisticated cybercriminal may one day successfully hack one of plaintiffs' vehicles. The court also found that the plaintiffs had not produced any evidence to support their claims that their vehicles were worth substantially less than the vehicles would be without the alleged cybersecurity defect. On appeal, the Ninth Circuit agreed in a short opinion, *Cahen v. Toyota Motor Corporation* (Casetext, 2017), reiterating that the alleged risks arising from the alleged vulnerability were speculative, and had never manifested. The court also concluded that the plaintiffs has failed to sufficiently allege an injury due to overpayment for their vehicles, noting that the plaintiffs did not, for example, allege "a demonstrable effect on the market for their specific vehicles based on documented recalls or declining Kelley Bluebook values," and they had not alleged "a risk so immediate that they were forced to replace or discontinue using their vehicles, thus incurring out-of-pocket damages."

Flynn v. FCA US LLC

While the Cahen case worked its way through the legal system, a journalist for WIRED magazine published an article demonstrating how several white hat hackers were able to take over control of the major functions of his 2014 Jeep Cherokee through its Internet-enabled infotainment system (Greenberg, 2015). The class action lawsuit *Flynn v. FCA US LLC* (Casetext, 2016), soon followed. Similar to the Cahen case, a large group of vehicle owners asserted numerous theories of recovery against the manufacturers of both the vehicle and the infotainment system. The plaintiffs claimed the vehicles were "rolling deathtraps" because the infotainment system had design vulnerabilities that allowed hackers to take remote control of the vehicle's functions, including the vehicle's steering and brakes. The defendants responded with a motion to dismiss, arguing that the plaintiffs had no standing to pursue their claims because the suit was based on a "hypothetical, speculative event" and there was no evidence that anyone, outside of the news article, had ever hacked and taken control of a Jeep Cherokee. The car-owner plaintiffs responded by arguing that they had suffered an injury because the cybersecurity weaknesses of the infotainment system diminished the value of their vehicles, and even though no catastrophic injury had yet occurred, the cars were

.

worth less than what they had originally believed they were purchasing (Trader, S. 2016).

The district court initially rejected the bulk of the motion to dismiss as premature, noting there were genuine issues of material fact about whether there was a true loss of market value for the vehicles, whether the alleged lack of cybersecurity constituted a legal defect, and whether a security patch for the software had cured the alleged defects (Casetext, 2018). However, after more than a year of additional discovery and legal wrangling, the defendants once again asked the court to dismiss the case for lack of standing. This time the court granted the motion, agreeing that there was no proof of actual injury or imminent injury (Casetext, 2020). The court noted that there was nothing that demonstrated a diminished market for the vehicles. There was no proof of declining Kelley Bluebook values and no proof that any of the plaintiffs had sold their vehicles at a loss due to the alleged defects. The court also stated that it was unclear whether the infotainment system was "defective at all," noting that just because there were vulnerabilities and the product could have been made safer, that "does not make it defective when no vehicles have ever manifested the alleged defect." (Casetext, 2020). The only time one of the 1.2 million vehicles had been hacked was the single occurrence noted in the WIRED article.

Unlike the high-profile products liability litigation of past decades that held manufactures liable for creating unnecessarily dangerous products and sparked lawmakers to create new regulatory agencies like the National Highway Traffic Safety Administration to ensure safer products, the products liability lawsuits based on IoT cyber-physical device security have quietly disappeared. These unsuccessful attempts to hold IoT device manufacturers accountable suggest that, at least in the short term, products liability litigation is not going to have the same profound impact on product safety as we have seen in other industries. The next section will discuss whether it is likely that there will soon be any progress.

WILL PRODUCTS LIABILITY LITIGATION ENHANCE CYBER-PHYSICAL DEVICE SECURITY?

The two published cases dismissing consumer attempts to hold manufacturers liable for weak IoT cyber-physical device security highlights at least four obstacles facing a plaintiff claiming that an IoT device manufacturer should be liable for producing a product with weak cybersecurity.

.

First, there must be a hacking incident where a plaintiff is actually injured.

Courts are reactive, not proactive. A court cannot act unless there is a proper case before it. As evidenced by the Cahen and Lynn decisions, speculative injury is not enough.

Second, it will be very difficult to prove that weak cybersecurity constitutes a defect in the device. As noted above, strict products liability in tort is the most prevalent theory of products liability litigation. In order to win a claim for strict products liability in tort, the plaintiff must convince the court that the product contained a defect. Defective products are those that fail to perform in the manner reasonably to be expected in light of their nature and intended function. What constitutes proof of a defect varies from state to state, but it generally requires proof that the product was designed, manufactured, or packaged in a manner that made the product unreasonably or unnecessarily dangerous. Products liability claims against IoT device manufacturers will most likely center on allegations that insufficient cybersecurity constitutes a defective design. To determine whether a product contained a defective design, courts focus on whether "the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design." (Restatement (Third) of Torts: Products Liability, 1997). The key term in this phrase is "reasonable alternative design." Plaintiffs must do more than merely allege that the product could have been safer, because virtually all products could be made safer. As noted above, automobiles would be infinitely safer if the passenger compartment was encased in lead, but that would be economically impractical. The question often boils down to a risk-utility test, which is essentially a cost-benefit analysis comparing the product's risk to its utility. A product is defective if a "reasonable person" would determine that the likelihood of seriousness harm actually outweighs the burden or costs of taking additional precautions. For example, the amount of cybersecurity necessary to safeguard the ignition system of a nuclear weapon is not equivalent to the amount necessary to secure the IoT functions of a coffee maker. While there may be a remote risk that a bad actor could overtake the control of an IoT coffee maker and start a fire, how much should be spent to make sure that coffee makers are safe from such an unlikely occurrence? Does the consumer expect topline on all consumer products, or is it expected that the network or router will be primarily responsible for defense? Because the only cases to address cyber physical device security were dismissed for lack of standing, no court has even reached the important risk-utility test. However, the District Court Judge in the Flynn case did openly question whether the fact that someone was able to hack the Jeep was even enough to prove that the cybersecurity was defective.

ISSN: 1941-6679-On-line Copy

.

Similarly, mere proof that an IoT product was hacked will likely be insufficient to prove that the product was defective because, as is often stated in the IT industry, everything connected to the Internet is vulnerable. This evokes an old exception to products liability discussed in the Second Restatement of Torts, which notes that some products are unavoidably unsafe. According to this doctrine, "There are some products which in the present state of human knowledge, are quite incapable of being made safe for their intended and ordinary use" and there can be no assurance of safety, so therefore the "seller of such products.is not to be held to strict liability for unfortunate consequences merely because he has undertaken to supply the public with an apparently useful and desirable product." (Restatement of Torts (Second), 1965). Products such as industrial-strength bathroom cleaners, acetone, benzene, and cosmetics like hair bleach, and dye are examples of unavoidably unsafe products that simply cannot, by their nature, be made safe and still fulfill their intended purpose. The design of the product packaging and warning labels can provide some level of protection, but ultimately the product will contain this unavoidable lack of safety. Because this doctrine is typically invoked for chemicals, it is unknown whether courts would expand this doctrine to include IoT devices. However, it is hard to deny that there will always be a certain amount of unavoidable risk whenever a product is connected to the Internet.

Third, beyond the defect, the plaintiff in an action for strict products liability in tort must also prove that the manufacturer's defect was the foreseeable cause of the injury. Proof of causation will be complicated because the hacker, not the IoT manufacturer, is the party that caused the injury. Manufacturers are normally excused from liability if a criminal intervened and caused the injury. This defense is not insurmountable because Scott provides examples of courts finding product manufacturers liable when the criminal intervenor was "highly foreseeable." (Scott, 2008). But it is not clear whether this rule would apply to IoT products. Does a general risk of a cyber-attack that impacts every device connected to the Internet make it highly foreseeable that a particular IoT device will be attacked? There are billions of IoT devices in the marketplace, and the lack of verified examples where a bad actor has overtaken an IoT device to cause property damage or personal injury undercuts any argument that such attacks are "highly foreseeable." Fear of cyberattack does not necessarily equal foreseeability. This area of the law has simply not been sufficiently tested in the realm of cybersecurity and it is very difficult to predict how courts will rule on this issue. However, because a hacker is the true cause of the damage, this criminal or tortious act by a third party could very well limit liability for the manufacturer, even though insecure code within the IoT device contributed to the risk.

ISSN: 1941-6679-On-line Copy

.

Finally, plaintiffs bringing strict products liability in tort claims often have to overcome the defense of assumption of the risk. This will be a formidable defense for IoT manufactures because if the IoT device manufacturer alerted its users of a potential vulnerability and a user continues to use the device before installing a patch, the manufacturer's liability could be reduced to zero. Similarly, if the user connected the IoT device to an unsecured network, the user might bare some or all of the blame for the cyberattack.

As mentioned above, strict products liability in tort claims are not the only legal theory available under the broad umbrella of products liability litigation. Plaintiffs often present the court with alternative theories of recovery that are not based on proof of a defect, but proof that the defendant was negligent or breached a contractual warranty. However, these theories also present several obstacles.

A plaintiff suing for negligence needs to prove that the defendant acted with a lesser standard of care than a reasonable person in similar circumstances would have acted. Therefore, a successful plaintiff would need to convince the court that the defendant failed to meet a standard of care, in this instance a standard of care for the IoT industry. As Amodio notes, there is no universally accepted industry standard of care for security in the IoT industry and legislators have been wary to establish one through statute (Amodio, 2020). Therefore, it would be very difficult to prove a failure to adhere to an amorphous standard. Also, because of rapidly evolving technologies and new methods to exploit those technologies, it will be very difficult to pin down any standard of care at any specific point in time. Other defenses applicable to strict products liability in tort will also apply to negligence. The plaintiff will need to prove there was an actual injury and overcome the fact that the injury was caused by a criminal hacker, not the manufacturer. Likewise, if the plaintiff did not keep current with any software updates for the IoT device, the claim may be lost because the plaintiff assumed the risk of injury. In short, if a plaintiff's claim of strict products liability in tort fails, any attempt to prevail under the alternative theory of negligence will most likely also fail.

Successful claims for a breach of warranty seem even less likely for IoT devices. With such claims, the plaintiff argues that the defendant violated the implicit or express warranties created by the contract for sale of the product. However, because these claims hinge on the existence of a contract, they are susceptible to the contract defense of waiver. Rustad notes how manufacturers can easily avoid significant contractual liabilities through simple End-User Licensing Agreements ("EULAs") where consumers agree to waive most damages in exchange for use of the product (Rustad, 2005). Oftentimes, EULAs specifically limit the plaintiff's remedies to the repair or placement of the product.

.

In total, it seems that plaintiffs attempting to hold manufacturers liable for producing IoT products with weak cyber-physical device security will face many legal hurdles that will at least significantly delay litigation in this area. As a result, it is unlikely that there will be any successful products liability lawsuits pertaining to cyber-physical device security in the near future.

CONCLUSIONS AND IMPLICATIONS

This article addressed two questions. First, whether there have been any successful products liability court decisions that have held manufacturers liable for creating IoT products with inadequate cyber-physical device security? Second, is it likely that products liability litigation will soon lead to significant change in IoT cyber-physical device security? Both questions were answered in the negative.

The analysis of existing products liability laws and how they are applied to new technologies illustrates a weakness in the current system. Each time a manufacturer is held responsible for failing to foresee dangers inherent in its product, the law becomes clearer and more easily applied to the next set of circumstances (Teret, 1981). The accumulation of enough such cases can compel real change in the industry. However, when a legal system faces new technology, it struggles to maintain certainty as the ramifications of the new technology are applied to existing principles, and changes may come slowly via a case-by-case basis (Harvey, 2017). This certainly appears to be the case for products liability and IoT devices. The lack of meaningful progress towards holding IoT manufacturers accountable for producing IoT devices with weak cybersecurity for non-data related devices means that the end is not in sight.

These findings have implications for IoT device users, device manufacturers, and the government agencies whose job it is to deter data breaches and other IoT-related cyberattacks. The primary implication for users is that they need to carefully weigh the benefits and consequences associated with the use of each IoT device. Over time, users should become more aware of these issues as they gain experience using the devices and see stories about device-related problems. All devices can be hacked, but there are a widely varying range of potential consequences. Unlike past phases in the Internet's evolution where private information or financial assets could be stolen, hacking connections to cars, homes, or wearable devices can potentially result in property damage or loss of life. The current IoT legal environment also has implications for IoT device manufacturers.

ISSN: 1941-6679-On-line Copy

.

If IoT device manufacturers do not fear products liability actions related to cyber-physical device security then they may continue to produce potentially dangerous devices that could harm users. They should know, though, that if the laws evolve as they have with other information technologies then they will be held to a higher standard over time. For legislators and the legal community, if there are no well-known instances of large liability, liability potential may not even attract the attention of decisionmakers. Without such instances, large liability costs cannot be recalled, and hypothetical costs seem harder to imagine than actual ones. Legislators will need to consult with technology experts to better understand the potential benefits and consequences associated with IoT device use in this rapidly evolving environment.

REFERENCES

Abomhara, M. & Køien, G.M. (2015). Cybersecurity and the Internet of Things: Vulnerabilities, Threats, Intruders, and Attacks. *Journal of Cyber Security, 4*, 65-88.

Alaba, F.A., Othman, M., Hashem, I.A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications, 88*, 10-28.

Amodio, L.M. (2020). The Intersection of Product Liability Law and the Internet of Things. *B.C. Intell. Prop. & Tech. F., 1*, 17.

Capano, D.E. (2021). Throwback Attack: Lessons from the Aurora Vulnerability. Control Engineering. Retrieved October 27, 2021, from https://www.controleng.com/articles/throwback-attack-lessons-from-the-aurora-vulnerability/

Casetext. (2013). Clapper v. Amnesty International U.S.A., 568 U.S. 398 (2013). Retrieved October 28, 2021, from https://casetext.com/case/clapper-v-amnesty-intl-usa-7?PHONE_NUMBER_GROUP=P&sort=relevance&p=1&type=case

Casetext. (2015). Cahen v. Toyota Motor Corporation, 147 F. Supp. 3d 955 (N.D. Cal. 2015). Retrieved October 27, 2021, from https://casetext.com/case/cahen-v-toyota-motor-corp-3

.

Casetext. (2016). Flynn v. FCA US LLC, Case No. 16-mc-00078 DGW (S.D. Ill. Nov. 30, 2016). Retrieved October 28, 2021, from https://casetext.com/case/flynn-v-fca-us-llc-2

Casetext. (2017). Cahen v. Toyota Motor Corp., 717 F. App'x 720 (9th Cir. 2017). Retrieved October 27, 2021, from https://casetext.com/case/cahen-v-toyota-motor-corp-2?PHONE_NUMBER_GROUP=P&sort=relevance&p=1&type=case&tab=keyword&jxs=

Casetext. (2018). Flynn v. FCA US LLC, Case No. 15-cv-0855-MJR-DGW (S.D. Ill. Jul. 5, 2018). Retrieved October 28, 2021, from https://casetext.com/case/flynn-v-fca-us-llc-8?q=Flynn%20v.%20FCA%20U.S.%20LLC&PHONE_NUMBER_GROUP=P&sort=relevance&p=1&type=case

Casetext. (2020). Flynn v. FCA US LLC, Case No. 15-cv-855-SMY (S.D. Ill. Mar. 27, 2020). Retrieved October 27, 2021, from https://casetext.com/case/flynn-v-fca-us-llc-13

Dean, B.C. (2018). An exploration of Strict Products Liability and the Internet of Things. Center for Democracy & Technology. Retrieved October 27, 2021, from https://cdt.org/wp-content/uploads/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf

Eads, G. & Reuter, P. (1983). Designing Safer Products: Corporate Responses to Product Liability Law and Litigation. Santa Monica, CA: The Rand Corporation. Retrieved October 27, 2021, from https://www.rand.org/pubs/reports/R3022.html

Garber, S. (1998). Product liability, punitive damages, business decisions and economic outcomes. *Wisconsin Law Review*, *1*, 237-296.

Greenberg, A. (2015). *Hackers Remotely Kill a Jeep on the Highway --with Me in It*, WIRED (July 21, 2015), Retrieved October 27, 2021, from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Harvey, D. (2017). Collisions in the Digital Paradigm: Law and Rule Making in the Internet Age. Bloomsbury Publishing Plc.

.

Johnson S.D., Blythe, J.M., Manning M., and Wong G.T.W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *PLOS ONE, 15(1)*.

Li, C., & Palanisamy, B. (2018). Privacy in Internet of Things: From principles to technologies. *IEEE Internet of Things Journal*, *6*(1), 488-505.

Llamas, M. (2021). Why We Need Mass Tort Lawsuits. Retrieved October 27, 2021, from https://www.drugwatch.com/lawsuits/why-we-need-lawsuits/

Maras, M.H. (2015). Internet of Things: security and privacy implications. *International Data Privacy Law*, *5*(2), 99.

Markey E. (2015). Retrieved October 27, 2021, from https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf

Mulligan, S.P., Linebaugh, C.D., Freeman, W.C. (2019). Data Protection Law: An Overview. Congressional Research Service. Retrieved October 27, 2021, from https://crsreports.congress.gov/product/pdf/R/R45631

Nash, I. (2021). Cybersecurity in a post-data environment: Considerations on the regulation of code and the role of producer and consumer liability in smart devices. *Computer Law & Security Review, 40,* 1-13.

Noor, M.B.M & Hassan, W.H. (2019). Current research on Internet of Things (IoT) security: A survey. *Computer Networks, 148*, 283-294.

O'Brien, H.M. (2015). The Internet of Things: The Inevitable Collision with Product Liability. Retrieved October 27, 2021, from https://www.productliabilityadvocate.com/2015/02/the-internet-of-things-the-inevitable-collision-with-product-liability/

Prosser, W.L., Wade, J.W. and Schwartz, V.E. (1988). Torts Cases and Materials, 8th edition.

Restatement of Torts (Second) (1965). § 402A. Special Liability of Seller of Product for Physical Harm to User or Consumer, Comment k. Retrieved October 27, 2021, from https://biotech.law.lsu.edu/courses/drugsf02/comment_k.htm

Restatement (Third) of Torts: Products Liability (1997). Retrieved October 27, 2021, from https://avemarialaw.libguides.com/c.php?g=265710&p=1777317

Rhode, D.L. (2004). Access to Justice, 35. Oxford University Press.

.

Rustad, M.L. (2005). The Tort of Negligent Enablement of Cybercrime, *Berkeley Tech. L.J., 20*, 1563.

Scott, M.D. (2008). Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?, *Maryland Law Review, 67*, 451-54.

Teret, S.P. (1981). Injury Control and Product Liability. *Journal of Health Policy. 2(1)*, 49-57.

Teret, S.P., & Jacobs, M. (1989). Prevention and torts: The role of litigation in injury control. *Law, Medicine and Health Care, 17(1)*, 17-22.

Trader, S. (2016). Drivers in Fiat Car Hacking Suit Say Their Injuries Are Real. Law360. Retrieved October 27, 2021 from https://www.law360.com/articles/774475/drivers-in-fiat-car-hacking-suit-say-their-injuries-are-real

Vailshery, L.S. (Mar 8, 2021). Internet of Things (IoT) and non-IoT active device connections worldwide from 2010 to 2025. Retrieved October 27, 2021, from https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

Valente, J., Wynn, M.A., Cardenas, A.A. (2019). Stealing, Spying, and Abusing: Consequences of Attacks on Internet of Things Devices. *IEEE Security & Privacy, 17(5)*, 10-21.

Vernick, J.S, Mair, J.S., Teret, S.P, Sapsin, J.W. (2003). Role of Litigation in Preventing Product-related Injuries. *Epidemiologic Reviews, 25(1)*.

Vernick, J.S, Mair, J.S., Teret, S.P, Sapsin, J.W. (2004). How Litigation Can Promote Product Safety, International and Comparative Health Law and Ethics: a 25-Year Retrospective. *Journal of Law Medicine & Ethics, Winter*, 551-555.

Viscusi, W.K. (2012). Does Product Liability Make Us Safer? *Regulation*. Retrieved October 28, 2021, from 309_Does-Product-Liability-Make-Us-Safer.pdf (vanderbilt.edu)

Wagner, W. (2007). When all else fails: Regulatory risky products through tort litigation. *Georgetown Law Journal, 95(3)*, 693-732.

Weber, R.H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review, 31*(5), 618-627.

.