This Internet Thing is Great, Isn't it, Hal? Product Liability in the Next 100 Years

By: Stephanie M. Rippee

Stephanie Rippee is a partner in the Jackson, Mississippi office of Watkins & Eager, PLLC. She has been a member of the IADC since 2009 and is a past Chair of the Product Liability Committee. Stephanie was an awkward teenaged girl, but in her advancing age has learned to embrace her "egghead" self, despite much good-natured ridicule from her husband and three sons. She has achieved the Certified Information Privacy Professional ("CIPP/US") designation from the International Association of Privacy Professionals ("IAPP").

I FALL into half of the readers that did not get Bill Anderson's reference to Hal in his introduction to this issue of the Defense Counsel Journal. I am no spring chicken. I was born in 1966 and have almost 30 years of law practice under my belt. But I was only two when *2001: A Space Odyssey* came out, and I have a general aversion to all things science fiction. So, I appreciated Bill's explanation, as well as his invitation to predict some trends in the direction of product liability litigation in the next one hundred (or maybe twenty) years. I chose data security as the focus of my "predictions."

I am a math lover, a college accounting major, and briefly considered tax school. Despite these facts, I have done a surprising amount of product liability litigation over the years. I live in Mississippi, which was a notorious litigation hellhole for years before we had a little tort reform. As a young lawyer, I was engulfed by a tidal wave of mass tort product liability litigation that swept through the state, primarily in the area of drugs and medical devices (as opposed to

asbestos, tobacco and a few other products that prompted mass tort tidal waves of their own).

Over the years, however, I have tried to maintain a balance of commercial litigation and product liability litigation in my practice. I have long had an interest in privacy issues which, in the past, normally involved economic losses and came up predominantly in my commercial cases. That appears to be changing. In the past 5-10 years, data privacy and security issues have exploded. They are impacting many areas of the law, including the world of product liability. The intersection of these two worlds is occurring primarily through what I call "smart products." I do not think it is rocket science (pun intended, Bill) to predict that issues arising from the use of smart products are going to reshape traditional product liability law and litigation in some ways over the next twenty (or maybe 100) years.

I want to back up and observe that as product liability law has developed over the past 100 years (with me witnessing almost thirty of those), the law seems to have done its job. Product liability law seems to have had the intended effect. Parties have been held accountable for unsafe products. Manufacturers, distributors and sellers have responded. Generally speaking, products seem safer today. I no longer see as many cases where a person loses a limb using a product that had inadequate safety guards, for example. Because of this, I think we have seen fewer "one off" cases. On the other hand, as Bill pointed out, we have seen a surge of mass torts, and many of them involve products we sometimes refer to as "unavoidably unsafe" or "inherently unsafe." They are good, safe products when used properly and accompanied by the proper warnings, but they cannot be made completely safe by virtue of their nature or function (e.g. drugs and guns). It seems to be easier for the plaintiffs' bar to make those good products seem "bad" in litigation. I wonder if mass torts involving smart products might become the next frontier for the plaintiffs' bar, whether that be in the form of "one off" cases or mass torts. It would not surprise me.

Technology seems to have played a key role in improving overall product safety. We now have smart products that can keep you from backing into another car or overdosing on medication. That is an upside of technology. As a downside, software glitches that cause malfunctions in product hardware can result in injuries to people (e.g., implantable heart devices like pacemakers).

Software malfunctions in smart products have definitely affected product liability law mostly by making cases more complex. But software glitches seem to be a topic for another article on another day. This article is focused more on data security issues as another one of the downsides of the incorporation of technology into products.

The intersection of data security issues with product liability litigation is still pretty new. The terms can be confusing. Different people use different terms for the same things. I think a little background is helpful to frame the issues. I am not providing you "the" definitions of these terms and ideas. I am providing you with my current thinking on them.

I. Smart Products, Connected Products and the Internet of Things

Products have evolved significantly over my career. I started practicing law when the internet did not exist, or at least was unknown to the general public. Lawyers did not even have computers (those were for their assistants) until about my sixth or seventh year of law practice. No one used email. Today, when our computers systems go down, we complain that it is impossible to work. We are that dependent.

Computer technology has by now found its way into everyday products. "Smart products" arrived on the scene first. I think of "smart products" as autonomous products that incorporate some type of software that allows them to be programmed (by a human) to improve function or efficiency. An example is a thermostat you can program to maintain temperatures at certain times of the day while you are not at home. Next came what I call "connected products." These are basically smart products that can be remotely controlled and monitored. Most smart products now seem to also be connected products. For example, now, you can control that thermostat remotely from an app on your phone. The internet connection that allows you to connect to connected products is vulnerable to hacking by a third party and creates what seems to me to be the primary intersection point between data security issues and traditional product liability litigation.

Now we also have the "Internet of Things" ("IoT"). To me, this refers to the now billions of everyday products s (e.g., your thermostat, your washer, your watch, your doorbell) that are connected to computers and/or

to other products through the internet. These products collect and analyze your personal data in real time without the need for human input (e.g., your Apple Watch). These products use and report personal data to a computer owner that both stores the data and analyzes it for various purposes including improved/ customized product function or service for you. The internet connections among IoT products, which again can be hacked, further amplify the intersection between data security issues and traditional product liability litigation because they increase the type and amount of data flowing back and forth over the internet. Reports vary, but supposedly there are now more than 20 billion devices that make up the IoT.

Regardless of these seeming distinctions, most smart products are now also connected products and many are also part of the IoT. As a result, I often see people (me included) use the term "smart product" as a good short-hand term to describe any product that incorporates any amount of technology (so, connected products and IoT products too).

II. Data Privacy and Data Security

Privacy and security are traditionally two different concepts. In the world of computerized data and the internet, these issues are converging somewhat as the harm we aim to prevent is the same: unauthorized access. Unauthorized access to online data is serious threat to both our privacy and our security. Thus, people often speak of "data privacy and security" in the same breath. Nevertheless, I think it helps to understand the difference between these concepts when looking at the future impact on product liability law.

Privacy focuses on how you (the product manufacturer, seller or distributor) use the data you gathered from me. Are you using my data for some purpose that would not be obvious to me from my decision to buy your product (meaning I likely did not consent to that use)? Are you selling it to another person or entity without my consent?

Security on the other hand focuses on making sure that you (the product manufacturer, seller or distributor) keep safe the data you gathered from me as I purchased and then used use one of your smart products. I have a right to expect that while you

have control over my data, it remains safe and is not accessed by a third party (e.g., a hacker) who could use the data to hurt me. Here, the distinctions blur somewhat because the company's inadequate data security could also be a threat to my privacy.

With the advent of laws like the General Data Protection Regulation ("GDPR") in Europe and California Consumer Privacy Act ("CCPA") in the United States, we are entering a new era in data privacy. These laws are "new" (broadly speaking) in that they allow consumers (i.e., product purchasers) to ask a company to identify the data the company has stored about that consumer and to describe exactly how the company has used or is using that data. They also generally allow consumers to control the further use or sale of their data (e.g., opt out of the sale of the data). Already, states like Nevada and Washington are following California with their own versions of this type of law. More states will follow. This patchwork of state laws will create an entire universe of new legal issues with which our traditional product liability clients will have to grapple. But those trends seem to be outside of traditional product liability litigation and thus also a topic for another article on another day.

Data security, synonymous in the digital world with "cybersecurity," seems to be the area that is having and will continue to have the most impact on traditional product liability litigation. Traditional product liability litigation is centered on trying to determine: 1) is there a defect in the product; 2) did it cause the alleged injury; and 3) who in the chain of manufacturing, distribution and sales is responsible for any harm caused by the defect? The joining of computer software, internet connections and products will impact these questions. This area of the law is new and rapidly changing. I do not think I can forecast any future trends except to say I expect a continued, significant increase in the effect data security issues will likely have on traditional product liability litigation.

III. Issues to Consider

I think the best I can do in this article is to try to preview some of the issues that may arise and have to be navigated. In other words, this article is going to provide you with questions, not answers. That might not be very satisfying, but I hope it is interesting and/or insightful. I do think it is a safe bet that, generally speaking, the law will develop and adapt in ways that continue to allow injured

consumers to recover damages from manufacturers, suppliers and distributors. I think this will be true even when a third party (i.e., a hacker) seems to be the party primarily to blame for the problem.

A. Product Defect

Is the vulnerability in the product connected computer system that a hacker intentionally exploits (i.e., the lack of data security in your product) - a "product defect"? For example, suppose a third-party hacker hacks into your "smart car" and disables the brakes, resulting in a crash that injures you and damages your car. Is the car defective in the traditional product liability law sense of that term? Courts have traditionally held that software is a service not a product. If a service rather than a product is at fault, traditional product liability law surrounding "defects" seemingly would not apply. But as software becomes more and more integrated into product hardware, (i.e., as software controls or changes the nature of the hardware more and more), it becomes more difficult to determine where one ends and the other starts.

If the software is deemed part of the "product," are software security vulnerabilities an inherent characteristic of any smart product? Generally speaking, it seems nearly impossible to design a software program with no vulnerabilities. Is this akin to the idea that it is impossible to design a drug with no side effects? All software seems to have bugs that later get "patched." As smart products and hacking become more commonplace, do consumers assume the risk of hacking? At some point, should the risk of third-party hacking of a product be considered open and obvious? That may depend on the product and the consumers using it.

With respect to "failure to warn" defects, knowing that it seems impossible to design perfect software, does a manufacturer that includes software in its product have a duty to warn consumers of the potential security vulnerabilities of the software? Is a manufacturer's failure to warn of software vulnerabilities a product defect itself? Does the manufacturer's duty of care extend to warning about the risks of third-party hackers? Traditionally, one would think no. Who knows if that will hold true in the context of smart products?

With regard to breach of warranty as a product defect, will the typical (fairly restrictive) end-user licensing agreements that seem to come with all smart products essentially eliminate

this type of defect as a form of recovery? These agreements usually disclaim liabilities stemming from software failures. Will or can those disclaimers be extended by manufacturers to the risks of hacking?

B. Standard of Care

If software is part of the product (not a service), what standard of care will be used to judge whether "defect" exists? What type of defect will a security vulnerability be classified as? It seems logical that a software vulnerability would be a design defect, but with computer technology, the line between manufacturing defect and design defect may not be as clear.

Under most state law, the type of defect affects the applicable standard of care. In Mississippi, for example, under the applicable product liability statute, a manufacturing defect claim is subject to a strict liability standard while a design defect claim is subject to a negligence standard.

If a software security vulnerability is classified as a design defect, it seems that the difficulty or ease of proving the defect will continue to depend, in part, on whether your state applies a consumer expectations test, a risk-utility test, or some hybrid or combination of the two.

C. Proximate Cause

Carrying the example forward, what proximately caused the injury – the intentional act by the hacker or the inadequacy in the product software that allowed it to be hacked? Was the hack an intervening, superseding cause? Or was the hack foreseeable to the product or software manufacturer? Proximate cause may be somewhat of an uphill battle for plaintiffs and thus an effective weapon in the defense arsenal.

D. Responsible Party

If the software vulnerability that allowed the hack is deemed a "product defect," and the hacker, the software designer and the product manufacturer can all be held partially responsible, there will be allocation of fault issues. To the extent a product manufacturer contracts with a third-party company to provide software for the product, manufacturers are going to want to position themselves as best they can, through contractual arrangements, to shift blame to the software provider. But as to the hacker with whom there obviously will be no contract, can the manufacturer ask the court to apportion fault? The hacker, after all, seems to be the real culprit

here. Under Mississippi, law, the answer to this question is no. With one small exception not relevant here, fault cannot be apportioned to intentional tortfeasors.[1] State laws on this issue surely vary. Statutes like Mississippi's make it more likely that the risks of damages from a product hack will be borne by manufacturers.

IV. Conclusion

I have really just scratched the surface of thoughts on how smart product data security issues will affect product liability law. With Hal at the helm, I think it is safe to say that people are going to become more and more dependent upon smart products, and the intersection of data security law and product liability law is only going to increase. Traditional product liability law will have to catch up and adapt. In what shape or form will that happen? Who knows?

[1] MISS. CODE ANN. § 85-5-7(1).