

For The Defense™

April 2018

driTM
The Voice of the
Defense Bar
The magazine
for defense,
insurance and
corporate counsel

PRODUCT LIABILITY

page 38

Including

**Traditional
Product Liability
Law and
Emerging
Technologies**

And More

Also in This Issue

**PROFESSIONAL
LIABILITY**

page 20

**ALTERNATIVE
DISPUTE
RESOLUTION**

page 72

|||||

*****CAR-RT LOT**C033
343521
MATTHEW D. GURBACH
BENESCH FRIEDLANDER COPLAN & ARONOFF LLP
200 PUBLIC SQUARE STE 2300
CLEVELAND OH 44114-2378

5807 P-3 P241

*Twenty Years of
Leadership at DRI:
An Interview with
Executive Director
John R. Kouris* page 3



New Questions in a New World

By Dawn Beery
and Kevin Burns

Among other things, the laws as they stand now will make a successful case harder and more expensive to make, and large-scale data breaches compromising safety may lead courts and legislators to consider reshaping them.



■ Dawn Beery is a partner of Benesch Friedlander Coplan & Aronoff LLP. Working in the litigation department out of Benesch's Chicago office, Ms. Beery focuses her practice on commercial litigation and product liability. Her product liability practice includes the defense of consumer products, industrial products, pharmaceutical products, and medical devices. Kevin Burns is an associate with Benesch Friedlander Coplan & Aronoff LLP. Working in Benesch's general practice group in Benesch's Indianapolis office, Mr. Burns focuses his practice on commercial, real estate, and intellectual property litigation.

The Application of Traditional Product Liability Law to Emerging Technologies

Product liability is one of the most expansive and varying areas of tort law in the United States. In 1965, the American Law Institute (ALI) drafted the Restatement of the Law, Torts 2d. Among its many provisions was

Section 402A, entitled, "Special Liability of Seller of Product for Physical Harm to User or Consumer." This model code section set the foundation for today's product liability laws. Section 402A states,

One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if, (a) the seller is engaged in the business of selling such a product, and (b) it is expected to and does reach the user or consumer without substantial change in the condition in which it was sold.

Restatement (Second) of Torts, §402A (2nd 1979).

Coincidentally in 1965, a book authored by future presidential candidate Ralph Nader, entitled, *Unsafe at Any Speed: The Designed-In Dangers of the American Automobile*, was published. This pioneering book shed light on the emerging issue of manufacturers, especially car manufacturers, creating products with disregard for their inherent danger and reluctance to implement adequate safety measures. The subject matter of Nader's book underscored a groundswell occurring at that time, which coincided with the American Law Institute taking a close look at product safety, liability, and measures to protect the public. Section 402A, and its revision in the Third Restatement, would serve as a model for every state to enact its own version of product liability law.

The basic requirements for plaintiffs, across most jurisdictions, to prove a claim for product liability are some variation of showing two things: (1) the product was inherently defective or negligently made, and (2) the defect in the product or negligence in its creation caused the injury. Product liability statutes differ from state to state both in their exact wording and their implementation. For instance, states vary on the length of their respective statutes of limitation, the availability of a cause of action for strict liability, the standard of negligence, and the availability of punitive damage awards in product liability actions. In general, most plaintiffs can bring a product liability claim under theories of negligence, strict liability, and breach of warranty. Strict liability claims can be based on a design defect, a manufacturing defect, or a failure to warn.

In this article, we will look at how four new areas of technology fit into the traditional product liability framework. We will look at (1) self-driving and autonomous vehicles, (2) smart-home products, (3) wearable technology, and (4) smart-toy products. Each of these categories of new and emerging goods presents the current product liability world with new questions.

Economic-Loss Doctrine

One of the public's greatest concerns regarding these emerging technologies is the risk that sensitive personal information could be inadvertently disclosed or exposed by hackers. The headlines are full of articles regarding data breaches and the resulting risk of identity theft. It might seem natural that if an inadequately secure device results in a data breach, a consumer could bring a product liability claim against that product manufacturer for damages resulting from the data breach. This is likely not the case. Because data breaches typically do not result in physical injuries or property damage, but rather result in purely economic damages, product liability claims resulting from data breaches are generally barred by the economic-loss doctrine. This is not to suggest that victims of data breaches have no remedy. Consumers can bring data breach claims for violations of, among other things, state data protection statutes, violations of the Fair Credit Reporting Act, and state unfair or decep-

tive business practices statutes. The various causes of action available to victims of a data breach are beyond the scope of this article, which is intended to focus only on product liability claims.

The economic-loss doctrine is a judicially created doctrine (which in some states has been memorialized in a statute) that deals with the convergence of two distinct areas of law: the law of contract and the law of torts. While the basis of recovery in contract law is to give a party the benefit of the bargain and make up for *economic loss*, recovery in tort law is built on the idea of compensating a party for injury. Courts have decided, in nearly every jurisdiction, that loss to property that causes mere economic loss is not recoverable in tort. That is to say, the proud owner of a brand new car, who drives it home, exits the vehicle, and immediately witnesses his or her prize possession burst into flames, is limited to a contract claim rather than a tort claim. Courts have chosen to make this distinction because even though they recognize that "people need more protection from dangerous products than is afforded by the law of warranty," the ultimate result of extending product liability to areas that were not originally within its province would cause contract law to "drown in a sea of tort." See *East River S.S. Corp. v. Transamerica Delaval, Inc.* 476 U.S. 858, 866 (1986).

While states vary in the scope of their economic-loss doctrine, nearly every state recognizes some version of the economic-loss doctrine. The majority of states simply prohibit plaintiffs from recovering purely economic damages in tort. See, e.g., *Danforth v. Acorn Structure, Inc.*, 608 A.2d 1194 (Del. Supr. 1992); *Giddings & Lewis, Inc. v. Indus. Risk Insurers*, 348 S.W.3d 729 (Ky. 2011); Minn. Stat. §604.10; *Alloway v. General Marine Indus., L.P.*, 695 A.2d 264 (N.J. 1997). The minority rule followed by only a few states rejects the application of the economic-loss doctrine and permits a plaintiff to recover purely economic damages in tort. See *Farm Bureau Ins. Co. v. Case Corp.*, 878 S.W.2d 741 (Ark. 1994); Conn. Gen. Stat. §§52-572m(b), 52-572n(a) (stating that consumers may recover for "harm," which includes damage to the product itself). A number of states have rejected these two extreme

positions and instead follow an intermediate rule that adopts the economic-loss doctrine but includes a number of exceptions, such as permitting tort recovery for economic damages when there was a sudden or dangerous occurrence that endangered the consumer, or when there was a special relationship between the consumer and the manufacturer. See *Progressive N. Ins. Co. of Illinois v. Ford Motor Co.*, 259 F. Supp. 3d 887 (S.D. Ill. 2017); *J'Aire v. Gregory*, 24 Cal.3d 799 (Cal. 1979); *Washington Water Power Co. v. Graybar Elec. Co.*, 774 P.2d 1199 (Wash. 1989).

There are numerous other exceptions to the economic-loss doctrine, which are also beyond the scope of this article. The key takeaway is that product liability claims for data breaches will be barred in most states when the resulting damages are purely economic and do not include physical injury or damage to other property. To the extent that courts or state legislators want to expand consumer protections for data breaches, amendments or revisions to a state's economic-loss doctrine would be a reasonable starting place.

Self-Driving Cars

If one were to ask Elon Musk about when exactly the era of autonomous self-driving cars would arrive, he would respond, "now." Musk is confident on the matter. In an online Time magazine article on June 2, 2016, Lisa Eadicicco reported that Musk exclaimed to a crowd at Recode's Code Conference, "I consider autonomous driving to be a basically solved problem." While most of us still drive ourselves and are not "passengers" in an autonomous car, in Silicon Valley and other technology centers, autonomous cars are becoming more and more prevalent. This emergence of a brand new and paradigm-shifting technology has the potential to complicate how we assign blame and compensate the injured when, inevitably, something goes wrong. Before we discuss the future, we should look at the present.

According to the National Highway Traffic Safety Administration (NHTSA), there were 10,497 drunk-driving deaths, 37,461 total roadway deaths, and 3,450 distraction-related deaths on U.S. roadways in 2016 (<https://www.nhtsa.gov>). These numbers are not surprising to most. The

general population acknowledges that automobile travel is potentially dangerous. While there are some autonomous cars on the road, the vast majority of cars are still “manned” vehicles. When a crash occurs between two manned cars due to driver error, the ultimate allocation of fault is normally an analysis of “who” was at fault, not “what” was at fault.

■■■■■
With developing technologies moving us toward an automated future—one in which driverless cars are likely to become more and more common—the legal implications of fault and cost allocation are dramatic.

For example, let us say that Driver A strikes Driver B, totaling Driver B’s car and injuring Driver B. In most states, Driver B could sue Driver A under a traditional negligence theory. In this situation, it is easy to determine who to name as the defendant in Driver B’s complaint: the other driver, Driver A. In the vast number of car crash cases, the parties either settle or the insurance pays out up to the limits. Rarely do vehicular negligence cases make it all the way through trial and to verdict. Additionally, when the negligent driver is uninsured or underinsured, many claims are never brought because they are not financially viable. Bryant Walker Smith, *Automated Driving and Product Liability*, Mich. St. L. Rev. 1, 33 (2017). However, what happens if Driver A was not really a “driver?” Consider this example: Driver A is intoxicated and gets into his autonomous car, which hits Driver B. Who is to blame? If you ask Hakan Samuelsson, President and CEO of Volvo Car Group, the answer is simple: “us.” Mr. Samuelsson made waves

when he was quoted in an October 7, 2015, *Fortune* article as saying that “the company will accept full liability whenever one of its cars is in autonomous mode.”

With developing technologies moving us toward an automated future—one in which driverless cars are likely to become more and more common—the legal implications of fault and cost allocation are dramatic. If Elon Musk is right and we are destined to be passengers rather than drivers, the majority of the liability for accidents will be borne by new defendants. In place of a negligent driver, we will see a liability shift toward the manufacturers, software developers, data providers, and component suppliers as named defendants in product liability litigation. Smith, *supra*, at 45. This dramatic shift of liability from “individual drivers under negligence to manufacturers under product liability broadly,” will cause those charged with prosecuting, defending, and adjudicating these claims to tackle new issues. *Id.*

A threshold issue for product liability claims will likely involve the software that drives and navigates the autonomous cars. If it is determined that a malfunction in the software led to a crash, and a lawsuit is pursued for a product liability claim against the software developer, the question will be, “is the software even a ‘product’ for the purpose of product liability?” *Id.* While some courts state that “custom programming” is a service, and others have held that a contract for custom software is a contract for goods. Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come*, 67 Md. L. Rev. 425, 436 (2008).

Assuming that the customized computer software of a self-driving car is deemed a product for purposes of a product liability claim, a plaintiff will still need to show that the product was defective to make the prima facie case. In Indiana, for example, to establish a prima facie case for strict product liability, the first element is to prove that “the product is defective and unreasonably dangerous.” *Nat. Gas Odorizing v. Downs*, 685 N.E.2d 155, 160 (Ind. Ct. App. 1997). While this process seems relatively straightforward, the mechanics of demonstrating that a piece of novel and innovative software is defective and unreasonably dangerous is a tall order. Requiring a plaintiff to “demonstrate how and why

an automated driving system performed poorly and should have performed better could impose technical and financial barriers to many claims.” Smith, *supra*, at 51. The collection of data necessary to demonstrate a failure of a piece of software may be dispersed among various parties and nonparties alike. This type of technical and legal collection of information adds to the already large costs of demonstrating a defect. Requiring a plaintiff to meet this burden favors a defendant. However, defendants should be aware that “permitting the plaintiff to use the consumer expectations test, the malfunction doctrine, or *res ipsa loquitor* could make it easier to attribute undesirable outcomes to something within the automated driving system.” *Id.* at 52.

As the technology advances every day, it is safe to assume that driverless cars are destined to become part of our daily life in the coming years. The idea behind the push for autonomous cars is ultimately to promote safer roadways by removing the element of human error. *Id.* at 12. The transition will not be without speedbumps. As with all innovative ideas and technologies, the cutting-edge navigation and self-driving software will take time to perfect. As we remove more and more drivers from the road, when accidents happen in the future, claims will not be for driver negligence, but for product liability. Manufacturers will hope that as the burden of liability shifts to them, the sheer number of vehicle accidents will decrease as the human error component is eliminated. Essentially, manufacturers will be responsible for a growing amount of a shrinking pool of claims. *Id.* at 72.

This shift of liability toward the manufacturers of autonomous cars for product liability claims will undoubtedly see a surge in the prevalence of product liability insurance coverage. As Jeff Sistrunk of Law360 described in his August 5, 2016, article entitled, “Driverless Cars Will Fuel Surge in Product Liability Coverage,” the underwriters are taking a “wait and see” approach to how the legal and technical landscape will look in the years to come.

Smart-Home Products

According to a Gartner study, by the year 2020, there will be over 6.4 billion con-

nected “things” in use globally. These “things” make up what is known as the “Internet of Things” (IoT). The IoT is a term used to describe the network of devices, technology, vehicles, implants, and other items that have the ability to connect to the internet, send, and share data with each other. Coined by Kevin Ashton in 1999, the term IoT includes all the products that we use today to automate our homes, colloquially known as “smart-home” devices. These devices include, among others, automatic locks, thermostats, smoke and gas detectors, cameras, television and communication devices, motion detectors, and remotely activated appliances. These devices have changed how we live by automating many aspects of our daily routine, reducing energy costs, and providing new levels of safety and security for our home. However, these products also present unique challenges from a product liability standpoint. With so many of our homes becoming automated, the possibility for something to malfunction or become

the subject of a third-party hack becomes increasingly likely. The internet-accessible thermostat and the smart oven are hardware in the traditional sense of product liability. If a hardware component malfunctions, the process to ascertain causation and fault falls in line with traditional product liability. But what if the software malfunctions? The intangible and ethereal nature of software and how it is used to help IoT products communicate presents a unique challenge from a product liability standpoint.

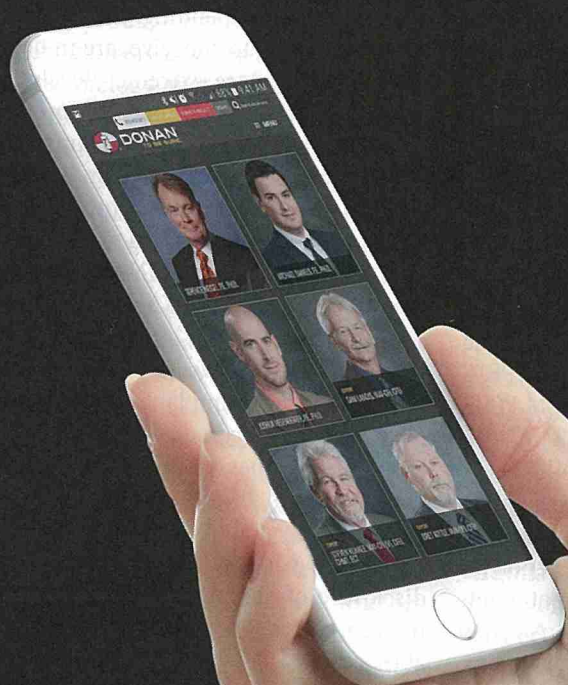
Let us take, for example, a smart oven. You are on your way home from work and use your smart phone to communicate over the internet to your smart oven to begin preheating. The software on the app allows you to set the temperature to 350 degrees. Alas, the software malfunctions and sets the oven to self-clean. Your entire home burns down and perhaps even causes bodily injury. Who is to blame? Depending on how the jurisdiction has determined whether a particular kind of software is a

product or a service, the software developer may be on the hook for a product liability claim. On the other hand, if the software is deemed a service and the consumer has no privity with the software developer, the consumer will be barred from bringing a product liability claim. To the extent that courts want to protect consumers and are reluctant to leave consumers with no remedy, courts in these IoT device cases may be more inclined to find software to be a product, rather than a service.

However, even if the software is decidedly a product and subject to product liability, there are several challenges. As discussed by Vincent Vitkovsky in his 2015 article, “The Internet of Things: A New Era of Cyber Liability and Insurance,” there are real challenges to mounting a negligence-based product liability claim for malfunctioning software for smart-home products. He states, “The collective, collaborative, iterative process of developing team-designed software in a breathtakingly fluid technological environment

EXPERTISE IN THE FIELD AND IN THE COURTROOM

Browse Donan's impressive library of experts at donan.com/experts or let us know what you're looking for at litrationsupport@donan.com.



DONAN
TO BE SURE. donan.com/litigation-support | 800-482-5611

will make it hard to establish a commonly accepted duty of care.” To prove that a software developer was negligent in its development of the software, a plaintiff must show that a vendor breached its duty of reasonable care by “failing to write or test the program properly, (2) correct significant bugs in the program, (3) warn of limitations in the program, (4) instruct users

It is foreseeable that any piece of software will have bugs in it; however, it is not foreseeable exactly how those bugs will affect the user of the software.

how to operate the program, or (5) provide adequate security for the system.” Lawrence B. Levy & Suzanna Y. Bell, *Software Product Liability: Understanding and Minimizing the Risks*, 5 Berkeley Tech. L.J. 1, 9 (1990). Plaintiffs have had a hard time successfully bringing these claims and proving them under a negligence theory. This is because proving the above-mentioned factors with a software product is both difficult and expensive. *Id.* at 10.

Instead of, or in the alternative to, a negligence claim, a plaintiff may opt to pursue a strict product liability action. In this case, a plaintiff would have to show that product defects were the proximate cause of the injuries or property damage. To make its case, a plaintiff must either show a manufacturing or design defect or a lack of adequate warnings. Showing a manufacturing or design defect can be difficult in the world of software for the same reasons previously discussed. Much of the software used in the world of the IoT is state of the art and expensive to investigate forensically. Additionally, to prove an actual defect is difficult because as a product, all complex software is understood to have “bugs.” It is foreseeable that any piece of software will have bugs in it; however, it is not foreseeable exactly how those bugs

will affect the user of the software. Scott, *supra*, at 443.

A final potential impediment to an end user being compensated through a product liability action for a malfunctioning smart-home device would be the end-user licensing agreements that accompany nearly every product. Smart-home product companies such as Nest, employ restrictive end-user licensing agreements, which disclaim all liabilities for the software failures of their product. The Nest end-user licensing agreement, as found on the Nest.com homepage, states:

NOTWITHSTANDING ANYTHING TO THE CONTRARY AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEST LABS PROVIDES THE PRODUCT SOFTWARE “AS-IS” AND DISCLAIMS ALL WARRANTIES AND CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, QUIET ENJOYMENT, ACCURACY, AND NON-INFRINGEMENT OF THIRD-PARTY RIGHTS. NEST LABS DOES NOT GUARANTEE ANY SPECIFIC RESULTS FROM THE USE OF THE PRODUCT SOFTWARE. NEST LABS MAKES NO WARRANTY THAT THE PRODUCT SOFTWARE WILL BE UNINTERRUPTED, FREE OF VIRUSES OR OTHER HARMFUL CODE, TIMELY, SECURE OR ERROR-FREE.

YOU USE ALL PRODUCT INFORMATION (AS DEFINED BELOW), THE PRODUCT SOFTWARE, AND THE PRODUCT AT YOUR OWN DISCRETION AND RISK. YOU WILL BE SOLELY RESPONSIBLE FOR (AND NEST LABS DISCLAIMS) ANY AND ALL LOSS, LIABILITY, OR DAMAGES, INCLUDING TO YOUR HVAC SYSTEM, PLUMBING, HOME, PRODUCT, OTHER PERIPHERALS CONNECTED TO THE PRODUCT, COMPUTER, MOBILE DEVICE, AND ALL OTHER ITEMS AND PETS IN YOUR HOME, RESULTING FROM YOUR USE OF THE PRODUCT INFORMATION, PRODUCT SOFTWARE, OR PRODUCT.

Because these end-user licensing agreements accompany so many IoT devices, the ability to bring a product liability action for breach of warranty is all but a moot point.

Wearable Technology

Much as with smart-home products, wearable technology is expanding at ever-increasing rates. Wearable technology refers to those devices that are worn by

a user and are connected to the internet, often using a Bluetooth connection to the user’s mobile device. The most common examples of wearable technology include smart watches and fitness trackers. While these devices do tell time or count your steps, or sometimes both, as you would expect, they also can alert you to incoming calls and texts, notify you of upcoming calendar appointments, monitor your heart rate while you exercise, and track you using GPS. Fitbit, Garmin, Polar, Apple and others have had varying degrees of success with these smart watches and fitness trackers.

Similar to wearable technology, implantable technology, also raises questions about the application of traditional product liability law to new technology. Today, implantable technology primarily consists of medical devices such as cardiac monitors, glucose sensors, and cochlear implants to improve hearing. These medical devices are used to monitor and treat chronic medical conditions, and their benefit is likely outweighed by any risk.

However, researchers are working on new types of implantable technology that are more for convenience than necessity. For example, implantable contraception chips that can be turned on and off by remote control, depending on whether a woman is trying to conceive, are in development. Even more extreme, developers in Australia have designed an implantable microchip that can be programmed to serve as your access key card for work and the gym, can open and even turn on your car, and can be programmed to obviate the need for passwords and PINs for everyday devices. See Simone Fox Koob & Ewin Hannon, *Shanti Korporaal’s Hands-On When It Comes to Tech Business*, The Australian, Aug. 3, 2017. Such implantable devices for convenience still come with their share of risks and will inevitably result in product liability claims.

As discussed above, the damages associated with a data breach that results in the disclosure of confidential personal information stored on wearable or implantable technology are likely not recoverable under traditional product liability theories because there is no physical injury or property damage, and so the claims are barred by the economic-loss doctrine.

To the extent that the consumers of these new connected wearables allege a personal injury, traditional product liability law will apply. For example, according to USA Today, at least one manufacturer of fitness trackers was forced to recall certain of its products because they were causing blisters and burns. See Mary Bowerman, *McDonald's Recalls 29 Million Fitness Trackers Amid Burn Reports*, USA Today, Aug. 24, 2016. Depending on the alleged injury, the difficulty that potential plaintiffs may face in bringing a product liability claim against the makers of wearable technology will be establishing causation. While it may be easy to establish causation in the case of a burn, causation of other types of injuries is much harder to prove. For example, plaintiffs who have brought product liability claims against cell phone manufacturers alleging that exposure to cell phones poses a cancer risk have struggled to establish that cell phone use caused or contributed to a consumer's cancer diagnosis. See *Newman v. Motorola Inc.*, 218 F. Supp. 2d 769 (D. Md. 2002), *aff'd*, 78 Fed. Appx. 292 (4th Cir. 2003). In the case of obvious injuries caused by wearable technology, established product liability law is appropriate to protect consumers.

The more difficult question is whether existing product liability law can adequately address a cyber-attack on wearable technology that results in personal injury or property damage claims, or both. For example, a hacker of wearable technology might be able to determine when a user sleeps, when that person goes to the gym, or when that person is out of the house. This information could then be used to harm the person or his or her property. Traditional product liability law will then be forced to address whether the manufacturer or its software developer, or both, took reasonable steps to secure users' personal data and prevent hacking. This inquiry will necessitate highly technical expert opinion from software developers and IT security professionals. Relatedly, the court will also have to determine whether the user can be found to be contributorily negligent if he or she failed to update the software for his or her device, or if the user set too weak of a password. These are issues that are yet to be addressed by the courts, but we can expect courts to con-

front these issues given the rapid growth in wearable technology.

Smart Toys

In an effort to cash in on children's love of technology, a number of toy manufacturers are now developing and selling smart toys. Some of these toys use Bluetooth connections to connect to a mobile device, and others record and store the parents' and child's information on the manufacturer's computer system. As with other online technology, these toys and their computer systems can fail or be compromised. As reported in a November 30, 2015, article in Law360, "VTech Hack Exposes 5M Parents, Kids' Personal Data," VTech Electronics admitted that its app store had been hacked and names, email addresses, passwords, mailing addresses, and genders and birth dates for both parents and their children had been compromised. Predictably, a group of parents and children filed suit against VTech for damages associated with an increased risk of identity theft stemming from the data breach. See *In Re: VTech Data Breach Litigation*, Case No. 1:15-cv-10889 (N.D. Ill.). This case was brought as a breach of contract action—not a product liability action—likely for the reasons discussed above.

Similarly, on February 28, 2015, Lee Mathews reported in a *Forbes* article entitled, "The Latest Privacy Nightmare For Parents: Data Leaks From Smart Toys," that seemingly innocent CloudPets had been hacked. CloudPets are stuffed animals that allow a friend or family member to record a voice message on the CloudPets mobile app and send it to the stuffed animal. The child can then send a response message by pressing a button on the CloudPet. The CloudPets data leak included voice messages and photos of children and adults who used the app. *Id.*

The safety and security of children's smart toys has also caught the attention of regulators and at least one legislator. On May 22, 2017, Senator Mark Warner of Virginia sent a letter, (viewable as a press release on the Senate website for Mark R. Warner) to the Federal Trade Commission (FTC) urging the FTC to do more to protect the safety and security of children using smart toys. While the Children's Online Privacy Protection Act (COPPA) was intended to protect children by mak-

ing the unauthorized collection, storage, and use of children's personal information illegal, many fear that it does not go far enough. Our natural inclination is to protect our children, and there is a pervasive sentiment that the current law does not go far enough. This may be an area where we will see product liability law evolve and expand to encompass claims

The safety and security
of children's smart toys
has also caught the
attention of regulators and
at least one legislator.

against a manufacturer that does not do enough to protect a child's data and personal information.

Conclusion

Since the inception of modern product liability laws in the mid-1960s, the goal has been simple: protect the consumer. In the post-war decades of the 1960s, as the American interstate highway system took shape and faster, more powerful cars flooded the roads, the laws reacted to keep people safe. Comfortably in the twenty-first century, we now look to what future products will bring in terms of convenience and potential harm. That potential harm is what our product liability laws will need to address. Dumb products are being replaced with smart ones. Cars are starting to drive us and not the other way around. In this new age of digital products, controlled by software, and able to communicate with each other in real time, 24 hours a day, there are a fair share of concerns to go along with the conveniences. Product liability laws, for the most part, are able to tackle these issues in their current form. However, the laws as they are written now will make a successful case harder and more expensive to make. Additionally, the increase in large-scale data breaches, some of which affect our children, may cause courts to reconsider the scope of product liability laws and how they should be shaped for the future.

