U.S. CHAMBER
Institute for Legal Reform

Torts of the Future II

Addressing the Liability and Regulatory Implications of Emerging Technologies

APRIL 2018

U.S. CHAMBER
Institute for Legal Reform

An Affiliate of the U.S. Chamber of Commerce

Table of Contents

Prepared for the U.S. Chamber Institute for Legal Reform by

Cary Silverman, Jonathan Wilson, and Sarah Goggans, Shook, Hardy & Bacon L.L.P.
In collaboration with Robert McKenna, Orrick partner and former Washington State Attorney General

Executive Summary

Emerging technologies are changing the way we live and work. Robots are moving from the factory floor to homes and businesses and they are increasingly able to "learn" and to make independent choices. At the same time, anyone with a 3D printer can become a product manufacturer, no assembly line required. As for our individual, human experiences, mobile devices monitor our health, movement, and sleep to help us achieve fitness goals. And we can visit a new place or an imaginary world with just a headset, smartphone, or eyeglasses. New technologies will undoubtedly improve lives, but they also come with new risks. How can courts and policymakers address legitimate safety and privacy concerns without derailing or delaying progress?

This second edition of "Torts of the Future" explores four emerging technologies: (1) robotics and artificial intelligence; (2) virtual and augmented reality; (3) wearable devices; and (4) 3D printing.

In each area, the report examines where the new technology stands in its development and the expected timeline for advancement. It then provides an overview of the existing regulatory and liability frameworks and how Congress, state legislatures, and government agencies are addressing these emerging technologies.

After providing this background, the report examines current and anticipated litigation. It considers such questions as: What types of claims are businesses in these markets likely to face? Do traditional liability principles adequately address risks stemming from the new technology? Are courts likely to alter these principles and expand liability? Is there significant potential for overregulation by Congress, state and local governments, and government agencies? And is there a need to place constraints on liability?

After exploring these areas, the report highlights recent developments in the technologies discussed in the 2017 edition of "Torts of the Future," including autonomous vehicles, commercial use of drones, private space exploration, the sharing economy, and the Internet of Things.

The report concludes by drawing from litigation and regulatory developments in each area to present guiding principles for addressing the liability and regulatory implications of emerging technologies.

Robotics and Artificial Intelligence

Once cordoned off from humans on the factory floor, robots are increasingly interacting with people in businesses and homes. As they gain the ability to learn and act independently, how will tort law respond when physical injuries, property damage, or other harms result?

Robots have long been used in industrial settings to perform such tasks as assembling products and moving inventory. Robotic technology is also used in hospitals, where it is closely controlled by surgeons. In these areas, robots function much like any other piece of workplace equipment or tool and courts have applied traditional principles of law.

As robots and other products become more capable of making decisions on their own, courts may look to alternative models of liability. Agency law may allow a robot to enter legally binding agreements on behalf of its owner. In other contexts, robots may be viewed in a manner similar to employees. Courts and legislatures may also look to principles of liability developed to address injuries from pets. In each of these areas, the person sued does not fully control the actions of the third party or animal that led to an injury, but, in some circumstances, is liable for the consequences.

Legislators could also give robots and other technologies with artificial intelligence a form of legal status that makes them responsible for their own actions and allows them to enter contracts and own intellectual property, much like corporations. The European Parliament is already considering making robots "electronic persons."

Virtual and Augmented Reality

Virtual and augmented reality devices and apps transport users to an alternative world. While this technology has exploded in the video game industry, it has a wide range of applications, such as allowing homebuyers to tour a home or helping doctors explore treatment options. These devices both increase existing risks of injury and lead to new liability concerns.

For example, if a person wearing a virtual reality headset does not create a safe area in which to use the device, then he or she can trip and fall over furniture, or hit a wall or ceiling. Or a virtual reality experience

"Once cordoned off from humans on the factory floor, robots are increasingly interacting with people in businesses and homes."

> *“[O]ne court is considering whether placing imaginary characters on private property can lead to a viable trespass or nuisance claim.”*

may be so frightening it causes a real-life heart attack. These and other types of hazards may be addressed by providing users with warnings of risks and adequate instructions for safely using the device, and by incorporating safety mechanisms into the products.

Augmented reality devices and apps, such as Pokémon Go, have been blamed for injuries and deaths caused by distracted drivers and by placing players in dangerous situations. Tort law, however, generally does not impose a broad duty on businesses that provide products or services to stop people from acting carelessly. Nor does tort law generally impose liability on a business for the criminal conduct of third parties, such as when a person who is staring into his or her phone late at night in a desolate area is robbed.

In some cases, these technologies will invite courts to apply existing principles of tort law to new situations or expand liability. For example, one court is considering whether placing imaginary characters on private property can lead to a viable trespass or nuisance claim. In the future, courts may be asked to address whether conduct that occurs in a virtual world, such as assault, graffiti, or theft, can give rise to real liability and, if so, who is responsible. Meanwhile, although courts have repeatedly rejected lawsuits that attempt to regulate violence in video games, new technology that makes the player a more active participant could inspire a new round of litigation.

Wearable Devices

In just a few years, wearable devices such as smart watches and fitness trackers have become mainstream and an integral part of many people’s daily lives. Wearable devices allow users to continuously track their vital statistics, location, and movement throughout the day and even while they sleep. With these devices, users can more effectively self-monitor their own health and potentially identify health issues.

While wearable devices can introduce significant benefits in terms of general health and personal convenience, the information they collect might also become important evidence in future litigation. Location, movement, and health information from these devices could be used to dispute claims related to personal injury or workers’ compensation, or even be used as evidence in a criminal trial.

In addition, due to the amount of health information these devices can collect, along with the potential lack of physician involvement in their use, manufacturers face potential legal and regulatory risks. The federal government and most states have thus far taken a balanced approach to regulatory and liability issues involving this technology. On the other hand, one state law, the Illinois Biometric Information Privacy Act, has resulted in an explosion of

> *[D]ue to the amount of health information these devices can collect, along with the potential lack of physician involvement in their use, manufacturers face potential legal and regulatory risks.*

consumer class actions, leading some companies to decide not to sell certain products in that state.

3D Printing

3D printing can turn digital blueprints into physical objects. As this technology becomes commonplace in businesses and homes, the public will gain access to custom products with the click of a button. From medical devices and engine parts to coffee mugs and replacement organs, 3D printing is poised to bring about the next industrial revolution.

When an injury related to a 3D-printed product occurs, which principles of tort law apply? Courts will need to decide threshold issues such as whether computer-aided designs (CADs) are "products" and whether a company that uses a CAD to print a product qualifies as a "product seller" even if it would not traditionally be viewed as a manufacturer.

If the answer to these questions is "no," then lawsuits stemming from 3D-printed products may rely on negligence claims. Negligence law includes significant constraints on liability but has sometimes proved malleable. For example, plaintiffs' lawyers may attempt to impose liability on a company when someone copies its design and precisely replicates its product, and that product injures someone. Plaintiffs' lawyers may also target a company that designed a product but never made or sold it.

Thus far, there is little litigation related to 3D-printed products. What litigation has occurred has involved a straightforward application of tort and consumer law principles.

> *Courts will need to decide threshold issues such as whether computer-aided designs (CADs) are 'products' and whether a company that uses a CAD to print a product qualifies as a 'product seller' even if it would not traditionally be viewed as a manufacturer.*

> *The first reported lawsuit filed against an autonomous vehicle manufacturer suggests that plaintiffs' lawyers may attempt to impose liability by viewing autonomous vehicles as human drivers rather than as defective products.*

Other Emerging Technologies: Recent Developments

AUTONOMOUS VEHICLES

The first reported lawsuit filed against an autonomous vehicle manufacturer suggests that plaintiffs' lawyers may attempt to impose liability by viewing autonomous vehicles as human drivers rather than as defective products. While Congress considers legislation intended to ease the path for deployment of more autonomous vehicles, states are enacting laws governing them at a quick pace.

COMMERCIAL USE OF DRONES

A National Conference of Commissioners on Uniform State Laws committee is drafting a model law that would address tort liability and defenses associated with the use of drones. Meanwhile, state and local governments have continued to adopt regulations that restrict drone use, one of which was found to be preempted by federal law in 2017. The federal government continues to work with state, local, and tribal governments to develop and test technology needed for drones to operate safely.

PRIVATE SPACE EXPLORATION

Georgia is the latest state to enact legislation designed to attract companies to locate spaceflight operations by limiting their potential liability. Meanwhile, the Trump Administration reinstated the National Space Council, which is concentrating on streamlining regulations to reduce barriers to private space exploration. Bipartisan legislation pending in Congress would also advance this goal.

THE SHARING ECONOMY

The Federal Trade Commission (FTC) settled its first enforcement action regarding data security practices in the ride-sharing context. Ride-sharing and home-sharing services continue to face significant litigation.

THE INTERNET OF THINGS

With more devices collecting and sharing potentially sensitive data, the FTC is broadening its enforcement net to address concern over whether connected devices contain sufficient security measures. The FTC announced its first settlement arising from a data breach involving a connected toy. A court, however, rebuked the FTC by dismissing an action alleging that smart baby monitors were susceptible to hacking where there was no consumer harm shown. Speculative private lawsuits alleging that connected systems in certain automobiles are vulnerable have also hit a red light in the courts.

Guiding Principles for Addressing the Liability and Regulatory Implications of Emerging Technology

There is no one-size-fits-all approach to addressing liability and regulatory issues associated with emerging technology. The key is to strike the right balance between promoting innovation and entrepreneurship and addressing legitimate safety and privacy concerns. To achieve that goal, this report offers guiding principles for the consideration of courts and policymakers.

Robotics and Artificial Intelligence

Robots and other products that are programmed to learn, make choices, and act independently have already arrived. In the foreseeable future, they will become commonplace. When their choices and actions are blamed for physical injuries, property damage, and other harms, lawsuits inevitably will follow. How are companies, courts, and governments addressing these issues? Are current common law principles adequate to address tort claims that arise from human interactions with autonomous robots and other products with artificial intelligence?

The late world-renowned physicist Stephen Hawking warned that as artificial intelligence (AI) reaches a level where it outperforms humans, "we cannot know if we will be infinitely helped by AI, or ignored by it and side-lined, or conceivably destroyed by it."[1] Similarly, Elon Musk, the CEO of SpaceX and Tesla Motors, has sounded an alarm, advising government officials that AI poses a "fundamental risk to the existence of human civilization."[2] Musk warns that AI poses "vastly more risk" than North Korea[3] and that it may be too late to respond if regulators wait "until people see robots going down the street killing people" to adopt safeguards.[4] Perhaps of more immediate concern, cybersecurity experts worry that, in addition to robots developing a mind of their own, they can be hacked, controlled by third parties, and told to do harm.[5]

As autonomous robots and other products with AI make their way into the workplace, provide medical care in hospitals, operate on public highways, and serve us in our homes, hotels, and stores, they will be involved in incidents that result in personal injuries and other harms. Lawsuits inevitability will follow, and the legal system will wrestle with how to assign fault in order to compensate the injured person and allocate associated costs.

Arrival of the Robots

ROBOTS IN THE WORKPLACE

Robots and automation in the workplace, of course, are not a new development. For decades, robots have assembled automobiles and other products in factories and moved goods in warehouses. Injuries and deaths associated with automated

machines occasionally happen. These incidents typically occur during human intervention, such as when a worker who enters the robot's "cage" accidentally activates it during a repair or other troubleshooting.[6]

The first reported death at the "hands" of a robot occurred in 1979, when 25-year-old Robert Williams was struck in the head by the arm of a five-story, one-ton machine at a Michigan auto factory, when he attempted to retrieve parts himself after the machine tasked with doing so malfunctioned. His death resulted in a $10 million jury verdict against the robot's manufacturer. A lawyer for the worker's family commented, "The question, I guess, is, 'Who serves who?'"[7]

Safety measures have improved to prevent such accidents, but they still occur. Among the latest reported fatalities is Wanda Holbrook, a 57-year-old technician who specialized in fixing robots at a factory that welded and stamped truck bumpers and trailer hitches. Holbrook died in 2015 after a robot "took Wanda by surprise," inexplicably moving from its assigned section of the plant into the area in which she was working. Upon entering the section, "the robot hit and crushed Wanda's head between a hitch assembly it was attempting to place in the fixture of [that section], and a hitch assembly that was already in the fixture," according to the 2017 lawsuit her husband filed against five companies that designed, built, and installed the robot.[8] Newspaper reports characterized the robot as going "rogue."[9]

These incidents are tragic, yet robot-related injuries and deaths are rare. According to Occupational Safety and Health Administration (OSHA) reports, about 30 workers suffered fatal injuries while working with robots over the past 30 years,[10] or about one death each year. To put this number in perspective, OSHA data indicate that approximately 5,000 workplace fatalities occur annually.[11]

Thus far, the lawsuits that follow robot-involved injuries or deaths assert the types of traditional legal theories that come into play when any equipment-related injury occurs in the workplace: allegations of design defects, such as the manufacturer's failure to incorporate a safety mechanism that would have avoided the injury; manufacturing defects; breach of implied warranty; failure to warn; and negligence, in addition to workers' compensation claims.

Robots imbued with AI will have functionality far beyond that of automated equipment and machines. They will move and act autonomously, make decisions and

> *"Autonomous robot interactions with workers will become commonplace and increasingly complex. The sheer volume of those interactions and their complexity will result in more accidents and claims. Theories of liability will evolve, precedents will be established, and both regulators and lawmakers will respond."*

learn from experience, and grow in capability beyond their initial programming. Their use and presence will expand beyond manufacturing to every type of workplace. Autonomous robot interactions with workers will become commonplace and increasingly complex. The sheer volume of those interactions and their complexity will result in more accidents and claims. Theories of liability will evolve, precedents will be established, and both regulators and lawmakers will respond.

In short, robots are being freed from their cages. Already collaborative robots, known as "cobots," are the fastest-growing segment of the robotics industry, projected to hit $135.4 billion in 2019, according to the tech research firm IDC.[12] Cobots are designed to function in tandem with human co-workers. In addition to their use in industrial settings, cobots may be found performing such everyday tasks as acting as security guards in the mall or making pizza.[13] Some Lowe's hardware stores have "LoweBots" roving the aisles, helping customers find what they need (in multiple languages) and tracking inventory.[14] These types of robots are generally cheaper, lighter, and more versatile than robots that operate in factories. They can be programmed by employees without robotics training. Some include AI. Importantly, some cobots are expressly designed to seek out and interact with the public, not to operate in isolation. If a worker or customer is injured, then all involved are potentially liable, including the cobot's manufacturer, its software developer, and its owner.

Some law firms are already advertising their services specifically to individuals who may have been injured by a robot at work. For example, a New York personal injury firm's website advises construction workers hurt by a robot to file both a workers' comp claim and a product liability action: "So, what you should really do if a robot injures you is talk to an attorney who has experience in both workers' comp and third-party liability suits. That way, you can choose the most advantageous strategy for recovering your rightful compensation."[15]

ROBOTS IN HEALTHCARE

In *The Empire Strikes Back* (1980), Star Wars introduced us to medical droids, including the 2B-1 surgical droid that treated Luke Skywalker after he was attacked by a Wampa and again after he lost his hand in a lightsaber duel with Darth Vader. Perhaps a future episode will explain what remedy a patient has in a galaxy far, far away when a surgery performed by a medical droid goes wrong. Today, on Planet Earth, surgical robots are a reality (as are robotic prosthetic hands) and the results aren't always perfect, whether due to flaws in the technology, decisions made by the humans trained to use them, or the unpredictability of medical outcomes.[16]

> *"[R]obots are being freed from their cages."*

Robots have proven advantages over human surgeons. They can operate with a level of consistency, precision, and steadiness that even the most skilled surgeon cannot match. They can also complete procedures less invasively, reducing the need for open surgeries that come with increased risk of complications, infections, and recovery time.

Today, robots used in medical procedures are closely controlled by human surgeons. For instance, the most common robotic surgery tool is Intuitive Surgical, Inc.'s da Vinci Surgical System. This Food and Drug Administration (FDA)-approved medical device serves as an extension of human doctors' hands, allowing surgeons who sit at a console a few feet from the patient to operate through small incisions rather than major cuts, and to make more precise movements. For over two decades, credentialed surgeons have used the system for laparoscopic surgeries to treat conditions in gynecology and urology as well as thoracic, cardiac, and general surgery.

As in other situations in which an error or bad outcome occurs during or after surgery, lawsuits have followed some procedures in which the da Vinci system was used. In fact, some plaintiffs' lawyers advertise on television and through the internet to generate claims alleging "robotic surgery malpractice."[17] As of late 2017, Intuitive Surgical was facing 43 individual product liability lawsuits and a multi-plaintiff case that includes 55 patients from 22 states.[18] Since these "robots" basically function as a high-tech tool, not as an autonomous replacement for an experienced surgeon, these lawsuits generally allege traditional medical malpractice claims against healthcare providers and ordinary product liability claims against the manufacturer. Plaintiffs may claim, for example, that the physician was not properly trained on how to use the device or warned of its risks. These cases, like any other medical injury case, have the potential for high awards.[19]

"While robotic surgery litigation to date has not involved products incorporating AI, medical device makers may face new liability that could be applied to such products."

While robotic surgery litigation to date has not involved products incorporating AI, medical device makers may face new liability as a result of such technology. In February 2017, after a jury returned a defense verdict, the Washington Supreme Court found that Intuitive Surgical had a duty to warn the purchaser of its device—the hospital that credentialed the doctor—of its risks.[20] The state high court ruling departs from the traditional application of the learned intermediary doctrine, which requires a company that makes a medical device or prescription drug to adequately inform the patient's *doctor* of the product's risks so that the doctor can talk with the patient about what might occur given that individual's medical condition. Had the case been re-tried, plaintiffs' lawyers would have tried to

convince the jury that the hospital, if properly informed of the risks of the technology, would not have allowed doctors to use it.[21] After the ruling, however, the case settled.[22]

Defense lawyers view the Washington decision as an outlier based on the specific language of Washington's Product Liability Act that other courts are unlikely to follow,[23] but plaintiffs' lawyers predict that "in 20 years, it will be well-established everywhere."[24] Manufacturers of medical devices express concern that allowing such a novel theory could chill innovation and interfere with the doctor–patient relationship.[25]

As surgical robots become less dependent on human doctors or even truly autonomous, plaintiffs are likely to rely on existing law as well as to try to further expand defendant liability. This type of technology is already on the horizon. Researchers have shown that robots can perform basic medical procedures. For example, the Smart Tissue Autonomous Robot (STAR) has proved capable of stitching tissue on its own. Researchers have tested the system, which is composed of a robot arm, suturing tool, and imaging system, on tissue harvested from pigs, finding that it can outperform surgeons. Eventually, the technology may play a part in some of the over 44.5 million soft-tissue surgeries performed in the United States each year. STAR's developers hope to move toward clinical trials, where they can show the technology's capacity to avoid human error and become smart enough to make adjustments when complications arise (e.g., excessive bleeding).[26]

Surgeries that use autonomous technologies will not occur until after the FDA has approved clinical trials and, eventually, regular use of such devices. Following FDA approval, when a bad outcome occurs, questions will arise about whether the surgical robot had defective hardware or programming, was improperly maintained, or was inadequately monitored. Such claims will be based on both product liability and medical malpractice law, and will focus on alleged design defects and user negligence. These cases, while complex, seem capable of resolution through applying traditional legal principles, just as in auto accident cases where the negligence of one or more drivers and the crashworthiness of the vehicle are at issue.

In addition, as the Washington Supreme Court case shows, plaintiffs' lawyers are likely to challenge whether the patient was properly warned of the risks of robotic surgery. When surgery is performed by a robot, plaintiffs might assert that the learned intermediary doctrine does not apply. Product liability experts observe, however, that when that scenario occurs, manufacturers of surgical robots will not simply "provide patients with instructions for use, tell them to 'have at it' and make up their own minds."[27] Rather, patients will continue to rely on medical professionals to explain the technology to them and obtain informed consent before its use. These medical professionals will continue to serve as the learned intermediary and the doctrine should continue to apply as traditionally understood.

ROBOTS AND AI IN THE HOME

Robots and consumer products that incorporate AI are being welcomed into our homes.

The 2018 consumer electronics trade show, held at the Las Vegas Convention

Center in January, was filled with "smart" consumer products, from refrigerators and other home appliances to televisions. Many products were advertised as designed to "talk" with Google Assistant or Amazon's Alexa. As explored in depth in the 2017 "Torts of the Future" report, connected products, known as the "Internet of Things," raise privacy issues, hacking concerns, and questions about the extent of a manufacturer's duty to address issues that may arise after selling the product.

The Las Vegas trade show featured robots that can take photos, remind the sick and elderly to take their medicine, and greet children at the door.[28] Some of the robots have hands capable of gripping objects or the ability to move and map a person's home, and they can learn faces, objects, and locations associated with objects—allowing them to fulfill a command such as "get me a beer" while also tidying up a person's house.[29] While vacuuming robots have long been available, robots capable of learning to perform these more complex tasks also now exist.

As autonomous robots become more common in and around the home, they will inevitably cause injuries or damage property. A Roomba knocking into a chair or running over a toe may not be cause for concern, but when a larger or more advanced robot or other AI product hurts someone while mowing the lawn, goes on an online shopping spree, breaks a neighbor's window, or drops a sick person it is moving from a bed to a wheelchair, litigation may result.

How Does Autonomous Technology Fit Within Existing Liability Models?

As products become more capable of learning, making decisions on their own, and developing their own "personalities," will existing legal principles prove sufficient to determine liability for injuries or resolve disputes? When such cases arise, plaintiffs' lawyers will look at everyone involved, including the inventor of the AI product, its manufacturer, and its owner. There is also movement toward providing AI entities themselves with a form of legal status, allowing them to enter agreements and be subject to liability for their own actions.

LIABILITY OF THE DESIGNER AND MANUFACTURER

At this point, when a robot or other product with limited AI (which some call "augmented intelligence") is alleged to have caused an injury as a result of a manufacturing problem or a design defect, or because of inadequate instructions or warnings, the designer, manufacturer, and

"As products become more capable of learning, making decisions on their own, and developing their own 'personalities,' will existing legal principles prove sufficient to determine liability for injuries or resolve disputes?"

seller may face a traditional product liability action. With respect to design defects, most state courts take a risk-utility approach, which considers whether the benefits of using a product as designed outweigh the risks of harm associated with the design. Whether a reasonable alternative design would have avoided the harm is often a key consideration.

Other state courts consider consumer expectations. This more subjective approach is vulnerable to erroneous judgments when by background and experience jurors can only speculate as to what a consumer might expect. Such guesswork does not result in sound decision making in cases involving highly complex products because consumer expectations regarding available safety features may be higher or lower than what technology allows, or may not consider how a product must be designed to maximize safety in a wide range of situations.

Manufacturers will have defenses available in these traditional product liability suits. Those that may be particularly applicable to cases involving robots or other products with limited AI include whether the product was altered or modified post-sale, or was misused in an unforeseeable or unreasonable manner (e.g., programmed or commanded to complete tasks for which it was not designed). Courts may also consider whether the user contributed to his or her injury by deliberately engaging in risky behavior under principles of comparative fault or an assumption of risk defense. A manufacturer may also protect itself from liability by providing adequate instructions for using the product, and by warning users of hidden dangers or risks that cannot be eliminated through an affordable and effective change to the product's design.

In the future, a key overriding issue with respect to robotics and AI will be whether a designer's or manufacturer's conduct can continue to be evaluated under product liability principles when a product is learning and changing after its sale. Should AI products be treated as "persons" rather than as "products?"

Manufacturing defects, which are deviations in the design of a product from its specifications, are subject to strict liability. While AI products may be identical "at birth," upon reaching the user, they may develop their own behaviors. Whether a product has a manufacturing flaw is evaluated based on its condition at the time of sale. This would preclude a manufacturing defect claim when an AI product was manufactured to design specifications but later changed.

The situation may be more complicated when evaluating whether an AI product's design is defective. By definition, AI products are designed to self-modify during

> *"Principles of law that have developed in the employment and animal-ownership contexts may provide a framework for AI owner or user liability."*

use. This may preclude a design defect claim. As products become more autonomous, traditional product liability law may fall to negligence principles, which might focus on whether the product's action was reasonably foreseeable and could have been avoided through exercising due care.

LIABILITY OF THE OWNER

Principles of law that have developed in the employment and animal-ownership contexts may provide a framework for AI owner or user liability. Both situations involve actions that are independent of the person sued but provide that a person may be responsible for injuries or other damage that occurs.

Robots as Agents. Agency is a relationship created by contract or by operation of law where one party, the principal, grants authority to another party, the agent, to act on behalf of and under the control of the principal to deal with a third party. Generally, the actions of the agent bind the principal.

For example, if a smart refrigerator orders food for the home or a robot nanny is manipulated into buying an expensive toy for the kids, under principles of agency law, a court may find that the owner is bound by such decisions. The technology may act, based on its programming, with either the actual (express) authority of its owner or, because the robot's action would give the impression to a reasonable person that it was authorized to act, with apparent authority.

The U.S. Court of Appeals for the Second Circuit has found that businesses can be bound by the actions of robots. In a 2004 case, a website design company, Verio,

"[I]f a smart refrigerator orders food for the home or a robot nanny is manipulated into buying an expensive toy for the kids, under principles of agency law, a court may find that the owner is bound by such decisions."

created an automated software application to identify new websites and compile the contact information of those who register the sites. The "search robot" would submit multiple queries to what is known as the "WHOIS" system, a publicly accessible database. Verio would then use this information to send marketing solicitations by email, telemarketing, and direct mail. The problem was that when receiving the results of a WHOIS query, users also received terms of use stating "that under no circumstances will you use this data to … support the transmission of mass unsolicited, commercial advertising or solicitation via email." Verio countered that it did not enter a legally enforceable contract when its search robot collected information from the database, among other reasons. The Second Circuit was not persuaded. It upheld a preliminary injunction against the company. While the court did not explicitly apply principles

> *[R]obots and other AI technologies may be viewed in a similar manner to employees.*

of agency law, it found that Verio was bound by the restrictions triggered by its search robots.[30]

Robots as Employees. *Respondeat superior* is Latin for "let the master answer." It generally provides that an employer is vicariously liable for the wrongful acts (torts) of an employee so long as the employee is acting within the scope of his or her employment. This doctrine most frequently comes into play when an employee gets into a car accident while driving a commercial vehicle or making a delivery in his or her own car. In such situations, the employer is liable for the employee's negligence. While the individual employee may have acted carelessly, the employer is nonetheless liable because it is viewed as benefiting from the employee's work, making it appropriate for the employer to shoulder the responsibility (through insurance or otherwise) for rectifying the harm.

Applying this lens, robots and other AI technologies may be viewed in a similar manner to employees. When a drone delivering a pizza hits utility wires that it fails to detect and crashes into someone on the ground below, a court might find that *respondeat superior* applies.

Would such liability discourage individuals or businesses from owning and relying on autonomous technology? For example, businesses have increasingly relied on independent contractors to reduce exposure liability that stems from the employer–employee relationship. Whether a person is an independent contractor or an employee turns on the level of control another person has over the worker's activities.

Might individuals similarly decide that rather than own robots, they will contract with a company that provides robot or other AI services, and maintains them, to limit the risk of liability? Could a "robot corporation" be created to exist independently, managed by the robots and financed through the services robots provide, effectively gaining legal rights?[31]

Robots as Pets. A person who keeps a wild animal as a pet is strictly liable for any injuries it causes because the behavior of the animal is unpredictable. On the other hand, liability for domesticated animals—pets—is more nuanced. Pets, like robots, are a form of property capable of making independent decisions and interacting with people. Pet owners have a general duty to prevent the animal from injuring others. Under common law, most jurisdictions have developed a "one bite" rule, which

> *Pets, like robots, are a form of property capable of making independent decisions and interacting with people.*

provides that when an owner knows that a pet has a propensity for viciousness, he or she is strictly liable for attacks. Some states have enacted statutes that impose strict liability for dog bites in particular situations or if the animal qualifies as a "dangerous dog" based on its breed. When a dog is provoked into biting a person, an owner may have a defense to liability. Owners of guard dogs who post warning signs may be able to reduce or avoid liability through the application of principles of assumption of risk or comparative fault.

Animals, while not human, are protected by law. Animal cruelty laws prohibit abuse that society has deemed morally reprehensible.

A robots-as-pets approach might appropriately balance owner responsibility, robot unpredictability, the level of risk of the particular robot based on its function, and the conduct of the person who was injured.[32] It also opens the door to providing legal protections for AI entities, when warranted.

LIABILITY (AND RIGHTS) OF THE AI ENTITY ITSELF?

As the discussion above shows, situations in the future may arise in which AI products act in a manner that is beyond the control of designers, manufacturers, or owners. In employment cases, for example, a business is generally not liable when an employee commits an assault. A pet owner may not be liable when a puppy that had always been gentle bites a four-year-old who enters its yard. Liability is based on principles of control, foreseeability, and fault.

One answer to situations in which the designer, manufacturer, or owner of an AI product is not liable under existing principles is to acknowledge that the purpose of tort law is not simply to compensate a person who has experienced an injury, but to do so when another party's wrongful action caused that harm.[33] Another option may be to recognize AI entities themselves as responsible for their own actions.

"[T]he purpose of tort law is not simply to compensate a person who has experienced an injury, but to do so when another party's wrongful action caused that harm."

Some suggest that the law will need to develop a limited form of "personhood" for autonomous technology that we will interact with in the same manner as people.[34]

"Some suggest that the law will need to develop a limited form of 'personhood' for autonomous technology that we will interact with in the same manner as people."

While some commentators posit "robot rights" that stem from their ethical or moral concern over a future form of conscious life,[35] at this stage in the development of AI technology, the motivation for providing autonomous technology with some legal status is largely driven by practical considerations. Corporations are "persons" under the law, and certain rights and responsibilities have been extended to them. Corporations are not individuals or human, but they have been granted many legal powers. Corporations can enter contracts, can sue and be sued, and are subject not only to civil liability but also to criminal penalties. They even have limited rights to free speech[36] and religious freedom,[37] and to engage in the political process.[38]

Providing AI entities with some form of legal status could provide assurance that an entity has authority to enter into legally binding contracts if, for example, it orders goods or services. Recognizing robots or drones as legal entities could protect the owner in situations in which the technology caused an accident while acting autonomously and the owner is not responsible for the action. The technology itself, supporters of this approach say, should carry its own insurance to cover claims. Limited personhood might also provide certain rights to AI entities, including the ability to own the intellectual property that it creates, such as software code and other technology, as well as art, music, articles, stories, or books.

Corporations have these rights already; they are in turn owned by individuals or by other corporations or entities, which ultimately are owned by individuals. Those owners benefit financially from the corporation's intellectual property and other property rights. Like corporations, which possess legal rights, it seems likely that AI entities with property and other legal rights will also be subject to ownership, and that their owners will also be the ultimate financial beneficiaries.

One country, Saudi Arabia, has jumped ahead, granting citizenship to a humanoid robot named Sophia, which was designed by a Hong Kong–based company to resemble Audrey Hepburn.[39] This appears to be more a publicity stunt than a decision intended to provide it with legal rights or responsibilities.

More serious consideration is occurring in Europe. In February 2017, the European Parliament voted in favor of moving toward recognizing autonomous robots as "electronic persons."[40] This recommendation was part of a broader resolution that created an ethical–legal framework for robots, but, predictably, it was this element that drew the most sensationalist media coverage.

The European Parliament's general recommendations, expressed in a resolution to the EU's Commission on Civil Law Rules on Robotics, include directing designers, producers, and operators of

"In February 2017, the European Parliament voted in favor of moving toward recognizing autonomous robots as 'electronic persons.'"

autonomous, self-learning robots to follow "Asimov's Laws,"[41] adopting codes of ethics for robotics engineers and researchers, and taking a "gradualist, pragmatic and cautious approach" to future initiatives to protect innovation.[42]

With respect to civil liability, the European Parliament's resolution finds that legislation should not restrict or limit compensation to an aggrieved person "on the sole grounds that damage is caused by a non-human agent."[43] "In principle," the resolution states, "once the parties bearing the ultimate responsibility have been identified, their liability should be proportional to the actual level of instructions given to the robot and its degree of autonomy, so that the greater a robot's learning capability or autonomy, and the longer a robot's training, the greater the responsibility of its trainer."[44] The Commission finds that, at this point, "responsibility must lie with a human, not a robot."[45]

The resolution recognizes, however, that when robots reach a level of autonomy and sophistication where their actions cannot be traced back to a specific person or entity, such as the designer, manufacturer, operator, owner, or user, and where the robot's actions were not foreseeable, traditional principles of liability may become insufficient. For that reason, the resolution calls on the Commission to explore the following:

- Whether to take a strict liability approach or impose liability on the person who is in the best position to minimize risks and deal with negative impacts in future legislation governing robot-related damages;[46]
- Establishing a classification and registration system for advanced robots, possibly grouping them by task, the environment in which they operate, their form, their level of human interaction, and their degree of autonomy; and[47]
- Developing a compulsory insurance scheme similar to auto insurance and creating a fund that would guarantee compensation for any damage caused by a robot that is not covered by insurance. A designer, manufacturer, programmer, owner, or user who contributes to the fund and has insurance coverage would be subject to limited liability.[48]

The resolution recommends considering specific issues and concerns related to autonomous vehicles, drones, robots used during surgery, "care robots," and medical robots.[49]

The most controversial recommendation is to give the most sophisticated autonomous robots "a specific legal status … in the long run," making the robots "electronic persons" responsible for any damage their decisions or interactions with people may cause.[50] Those involved have explained this

> *"The most controversial recommendation is to give the most sophisticated autonomous robots 'a specific legal status … in the long run,' making the robots 'electronic persons'…"*

recommendation as similar to corporate personhood—creating a new "legal fiction" as a tool of convenience—not akin to human rights. "Robots are not humans and will never be humans," declared Mady Delvaux, the Luxembourgish member of the European Parliament responsible for presenting the action to the public.[51]

The European Parliament's 2017 resolution does not have any legal force. This year, however, it may begin to vote on specific proposals to regulate robots and AI.[52]

Others question whether robots need "personhood."[53] Many animals have skills that are on par with or more advanced than current AI technology, but they are still considered property without personhood. For example, dogs help people with a wide range of medical conditions, search for people trapped after disasters, detect explosives, and respond to numerous commands. Other animals also have the ability to use tools, think, and create. In 2016, after lengthy litigation, a federal district court ruled that a "highly intelligent" Indonesian monkey named Naruto could not seek damages for copyright infringement when others published and sold selfies he took with a nature photographer's camera.[54] If a real monkey cannot create and own property, should an autonomous monkey robot have greater rights? Given the potential of AI entities to create intellectual property and other lasting value, the answer may be yes, as was decided long ago in granting certain rights to corporations and recognizing them as "persons" for certain purposes.

Virtual and Augmented Reality

Put on a headset, look into a smartphone, or wear a pair of special glasses and you can be transported to another world or view the world around you in a new light. Devices and apps that incorporate virtual and augmented reality technology make this possible but, at the same time, can be blamed for real-world injuries. As such incidents arise, courts will be invited to expand tort principles, particularly with respect to negligence, product liability, trespass, and nuisance law.

Virtual reality (VR) technologies fully engage people in an alternative world. The user's sensation that he or she has been immersed in an alternative reality is commonly achieved by wearing a headset plus sensors that track the user's movements. While wearing VR headsets, users are essentially blindfolded from the real world around them and placed in a digital environment where they interact with computer-generated objects.

On the other hand, augmented reality (AR) superimposes digital images and objects on the user's view of the real world. This is achieved through a smartphone, special glasses, or a headset. It is this combination of the real world and computer-generated graphics that distinguishes AR from the full-immersion experience of VR.

VR and AR technology have exploded in the video game industry. Nintendo's Wii in 2006 was an early foray into this area. While still relying on a standard TV set, the Wii allowed people young and old to play games ranging from tennis to bowling by tracking their physical movements rather than by relying on inputs from control pads or joysticks.[55]

A decade later, Niantic's Pokémon Go was a turning point for AR. Pokémon Go was the most downloaded iPhone app worldwide in 2016, reaching millions of people.[56] In this game, players take the role of "trainers" with the goal of capturing and collecting fantasy creatures known as Pokémon. Players use the features of their smartphone, including its GPS, camera, and gyroscope, to superimpose images over the camera's view of its real-world surroundings.

VR also had a banner year in 2016. Facebook-owned Oculus launched the Oculus Rift,[57] Sony first released its Playstation VR,[58] and HTC introduced the Vive.[59] The most sophisticated VR headsets, which are linked to video game consoles or computers, are generally priced in the $350 to $600 range.[60] Samsung and Google now make mobile VR headsets that are linked to smartphones and cost $100 or less.[61]

While VR and AR technologies are popularly known for their use in video games, they are also employed in a wide range of industries. For example, businesses have used VR for employee training, helping retail employees learn how to respond in common situations, and teaching construction workers to spot potential problems.[62] Realtors are providing clients with VR headsets, allowing them to save time by virtually touring houses.[63] VR is also used in healthcare. Physicians use VR to explore patients' internal organs and perform complex surgeries. Their patients are learning to use VR to control pain, treat anxiety, and help them recover from debilitating injuries.[64] VR technology is already being developed to diagnose medical conditions, such as brain injuries.[65]

Technology observers have declared that 2018 will be the "year of VR,"[66] with less expensive headsets, increased production and sales, a greater consumer comfort level with the technology, and new applications for its use. Others have less grand but high expectations, referring to 2018 as the year VR goes "cord-free" with new high-end standalone systems that are not tethered to game consoles or PCs.[67] Still, some predict that while a new generation of AR and VR devices will hit the market this year, the technologies will not reach their full market potential for another decade.[68]

New and Expanded Tort Liability Risks

CAN A PERSON WHO WEARS A VIRTUAL REALITY HEADSET RECOVER DAMAGES FOR INJURIES?

Observers predict that VR companies will face a surge of personal injury lawsuits brought by users who are injured while they or others are using a VR device.[69]

People wearing VR headsets can be prone to trip over cords, furniture, or other household objects; walk into or punch a wall; or fall down a flight of stairs. While throwing a virtual basketball, they may jump and hit their head on a chandelier or the ceiling. Users may also strike other people with a controller or damage property, particularly if they are playing a game that involves significant movements, like swinging a tennis racquet, kicking, or drumming. What may be the first reported VR-related death occurred in December 2017 when a 44-year-old man tripped and fell onto a glass table in his Moscow apartment while wearing a headset.[70]

"Observers predict that VR companies will face a surge of personal injury lawsuits brought by users who are injured while they or others are using a VR device."

> *"[M]anufacturers of VR devices have attempted to reduce their liability exposure by communicating clear safety instructions and warnings to consumers."*

While gamers may be careful to operate in a safe area and clear the space around them, what if a toddler or pet wanders into that area?[71]

Alternatively, an intense VR experience may be so frightening or exhilarating that it causes a heart attack or emotional trauma—consider the potential consequences of a simulated fall from a cliff. Engaging in actual or simulated movements through VR technologies may also have neurological and other physical effects on users. Some users have reported dizziness and nausea, for example.[72] In addition, there is a danger that flashing lights and patterns could trigger a seizure in a small percentage of people,[73] which for decades has led to personal injury lawsuits related to traditional video games.[74] These lawsuits have been largely unsuccessful, however, because they typically involve plaintiffs with preexisting medical conditions and, since the early reports of seizures, manufacturers have warned consumers of this risk.[75]

VR device manufacturers are likely to face product liability and negligence claims stemming from such injuries. These claims may allege that the device did not incorporate adequate safety mechanisms to warn the user of nearby people or objects; that the device lacked appropriate instructions, such as the amount of space needed to use the device safely; or that the manufacturer did not adequately warn of risks. It is also possible that, years in the future, plaintiffs' lawyers will allege that full-immersion VR experiences can cause neurological or cognitive harms.[76]

Thus far, manufacturers of VR devices have attempted to reduce their liability exposure by communicating clear safety instructions and warnings to consumers. For example, the Oculus Rift is accompanied by an extensive document that discusses potential hazards and how to avoid them. Here is a sampling of those instructions and warnings:

- "Virtual reality is an immersive experience that can be intense. Frightening, violent or anxiety provoking content can cause your body to act as if it were real. Carefully choose your content if you have a history of discomfort or physical symptoms when experiencing these situations."
- In rare cases, people may have "severe dizziness, seizures, eye or muscle twitching or blackouts triggered by light flashes or patterns . . . even if they have never had a seizure or blackout before or have no history of seizures or epilepsy."
- "This product should not be used by children under the age of 13" given the product's size and development concerns if used by young children.

> *Features that require users to consent to certain experiences or select or opt out of frightening, hazardous, or potentially offensive virtual content—such as violence, strobe lighting, or nudity—may enhance the user's experience while reducing liability exposure.*

- "Serious injuries can occur from tripping, running into or striking walls, furniture or other objects, so clear an area for safe use" before using the device.
- "Remember that the objects you see in the virtual environment do not exist in the real world, so don't sit or stand on them or use them for support."
- The device should not be used "near other people, objects, stairs, balconies, open doorways, windows, furniture, open flames, ceiling fans or light fixtures, televisions or monitors, or other items that you may impact when using…."
- "Take at least a 10 to 15 minute break every 30 minutes, even if you don't think you need it."[77]

Courts have generally found that providing these types of instructions and warnings preclude liability. For example, Nintendo won a lawsuit alleging that Wii remotes flew off users' wrists "like a missile" while playing the game—hitting people or damaging property—because the company had clearly warned of such risks and instructed users to not let go of the remote while playing the game.[78]

Providing adequate instructions and warnings, however, is not always enough to avoid liability. Plaintiffs' lawyers may point to a comment in the Restatement of Torts, Third: Products Liability, which recognizes that "[i]n general, when a safer design can reasonably be implemented and risks can be reasonably designed out of a product, adoption of the safer design is required over a warning that leaves a significant residuum of such risks."[79] In other words, some courts have adopted the principle that warnings are not a substitute for a reasonable, feasible safer design that would have reduced the risk of harm. For that reason, AR and VR makers will also need to incorporate safety features into their devices, such as alerts that detect nearby walls or objects. Features that require users to consent to certain experiences or select or opt out of frightening, hazardous, or potentially offensive virtual content—such as violence, strobe lighting, or nudity—may enhance the user's experience while reducing liability exposure.[80]

LAWSUITS ALLEGING AUGMENTED REALITY APPS CAUSE INJURIES BY DISTRACTED DRIVERS

Apps and devices that incorporate AR technology pose a similar, but distinct, set of risks as VR products. Unlike the VR user, an AR user can still see the surrounding world, but people immersed in an AR application may be distracted from real-world hazards. For example, they may be tempted to play an AR game while driving,

“Thus far, there are no reported lawsuits against Niantic or other AR app makers stemming from such distraction-related injuries, likely because such claims would face significant challenges in a court applying traditional principles of tort law.”

which poses similar and perhaps greater risks than texting and may lead to car accidents.

Pokémon Go reminds the user each time he or she plays: “Remember to be alert at all times. Stay aware of your surroundings.” Yet Pokémon Go has been blamed for injuries and deaths that have resulted while drivers and others are distracted by the game.[81]

Thus far, there are no reported lawsuits against Niantic or other AR app makers stemming from distraction-related injuries, likely because such claims would face significant challenges in a court applying traditional principles of tort law. Nevertheless, it is likely that AR app users and those injured by distracted drivers will bring lawsuits alleging that a technology’s manufacturer acted negligently by encouraging users to play or use an app while driving or alleging that a game or app designer could have incorporated safety features that disable it while the user is driving.

Tort law does not impose a broad duty on businesses that provide products or services to prevent people from acting carelessly while using them. For example, a federal district court dismissed a case brought against Google by a user of Google Maps who was hit by a car after the app’s directions suggested walking across a busy highway.[82] The lawsuit alleged that Google had a duty to exercise reasonable care in providing reasonably safe directions and a duty to warn users of dangers, such as cars traveling at high speed along a road. The court, however, found Google had no duty to the plaintiff, as it had no relationship with her beyond providing the same information made available to numerous others. It also recognized that “Google was not required to anticipate that a user of the Google Maps service would cross the road without looking for cars.”[83] Imposing a duty on the app maker, the court found, “would serve to diminish the responsibility that pedestrians have for their own safety…”.[84]

“Tort law does not impose a broad duty on businesses that provide products or services to prevent people from acting carelessly while using them.”

Drivers face numerous distractions—phone calls, text messages, screaming children in the back seat—but courts do not typically hold the source of the distraction, whether it be a person or product or app maker, liable for a driver's carelessness. For example, lawsuits have alleged that a person who sends a text message to someone who is driving is liable if an accident occurs. To date, these claims have not been successful,[85] but they are theoretically possible if there is clear evidence that a sender knew the recipient was driving at the time or had "special reason to know" that the person would view the text while driving.[86] That bar is not likely to be met with respect to designers of mobile applications.

Likewise, eating while driving is a leading cause of distraction and accidents,[87] but courts have not found restaurants that operate a drive thru liable for injuries or deaths caused by food-distracted drivers.[88]

Rather than expand tort law to impose liability on a third party tied to the source of the distraction, many state and local laws broadly empower law enforcement officers to ticket distracted drivers, whether it is because they are focused on a phone running an AR game or on a cheeseburger.[89] A savvy personal injury attorney will immediately search for evidence that a driver involved in an accident was texting, eating, or otherwise distracted when the accident occurred, to help establish the driver's negligence.[90] The law's focus should remain on drivers in such cases, since they control the level of their attentiveness or may allow themselves to become distracted. The alternative is to open the flood gates to lawsuits in which individuals injured by distracted drivers, and possibly the distracted drivers themselves, claim that businesses associated with any of numerous potential sources of distraction while driving are responsible for those who engage in risky behavior.

Plaintiffs' lawyers may have other creative theories to seek to impose liability on an AR app maker for car accidents. For instance, one personal injury lawyer compared Pokémon Go to a radio station that offered a prize to a largely teenage audience to be the first to catch a DJ who was constantly on the move.[91] When such a contest led to a "competitive pursuit" in which a participant negligently ran another vehicle off the road, the California Supreme Court upheld a jury award against the radio station for the family of a driver who died.[92] The court reasoned that it was foreseeable that young drivers would disregard highway safety and that the risk that a high-speed automobile chase could result in death or serious injury was unreasonable and should have been avoided.[93]

LAWSUITS ALLEGING AUGMENTED REALITY APPS LURED USERS INTO DANGEROUS SITUATIONS

News reports have also blamed Pokémon Go for luring people into dangerous areas or situations—which may occur with any AR technology in which users are distracted from the world around them.

People staring into their phones in unfamiliar areas are easy targets for criminals. There have been reports of game players robbed at gunpoint across the country.[94] In Missouri, three 18-year-olds were arrested and charged with using the app to rob at least 10 users at desolate spots that they knew would draw players searching for Pokémon.[95]

> *Tort law does not broadly require product makers, retailers, or others to prevent criminal acts by third parties.*

Tort law does not broadly require product makers, retailers, or others to prevent criminal acts by third parties. Absent exceptional circumstances, individuals are entitled to presume that third parties will not commit intentional criminal acts.[96] A store, for example, has a duty of reasonable care to protect visitors from reasonably foreseeable injuries at the hands of another, but courts often view criminal acts as intervening causes that break the chain of causation linking the harm to a negligent act on the part of a business.[97]

This general rule can be overcome if it is shown that a defendant knew or should have realized that a person would be exposed to a violent person or an atmosphere of violence.[98] Courts may also find a duty to protect a person from a criminal conduct when the defendant has some special relationship to the victim or the intentional conduct of the wrongdoer, or affirmatively took some action that created or exposed the person to a high risk of harm.[99]

Courts are likely to find, however, that holding a business liable for not taking sufficient steps to prevent a crime would be an exercise in "speculation and conjecture."[100] As courts have found in other contexts, tort law would send the wrong message if it conveyed that a perpetrator is not entirely responsible for an intentional criminal act.[101] These principles and policy considerations are equally applicable in the AR context.

Distracted AR app users may also place themselves in other types of dangerous situations. For example, a Florida homeowner shot at a pair of late-night Pokémon Go players whom he believed were burglars.[102] In Pennsylvania, a 15-year-old was hit by a car when she crossed a busy highway during the evening rush hour while playing the game.[103] In San Diego, two people fell from a cliff in pursuit of digital treasure.[104] As discussed earlier in the context of distracted driving, however, tort law does not impose a broad duty on businesses that provide products or services to prevent people from acting carelessly when using them.

> *As courts have found in other contexts, tort law would send the wrong message if it conveyed that a perpetrator is not entirely responsible for an intentional criminal act.*

CAN VIRTUAL REALITY GAMES LEAD TO TRESPASS OR NUISANCE CLAIMS?

Can images of cartoon characters "trespass" on private property or entice others to do so? Can an AR technology pose a nuisance to property owners?

Shortly after the release of Pokémon Go, a law firm known for securities class action litigation filed lawsuits against Niantic, claiming that Pokémon Go encouraged and rewarded trespassing on private land.[105] The three class actions were filed in a California federal court on behalf of anyone who owns property in the United States that was designated as a "PokéStop" or "Pokémon gym" or owns abutting property.

The lawsuits alleged that by placing virtual objects on or near private property without permission, Niantic directed game players to trespass, creating a nuisance. In the first case, a New Jersey man found strangers lingering outside his home and at least five gamers knocked on his door to ask if they could access his backyard to catch a Pokémon.[106] In the next case, a Michigan couple asserted that placement of a Pokémon gym and seven PokéStops in a small park across the street from their private cul-de-sac created a "nightmare" for them and their neighbors. The complaint alleged that a flood of visitors blocked their driveways, trampled their lawns, and peered in their windows, searching for Pokémon.[107] In the third case, a Florida condominium association claimed invasion by "out-of-control crowds" behaving "like zombies, walking around bumping into things" seeking rare Pokémon at "peak spawning hours," late at night and in the early morning.[108]

The lawsuits accused the company of "flagrantly disregard[ing] the foreseeable consequences of its game" by populating the real world with virtual Pokémon on or directly adjacent to private property, citing placement of PokéStops at the U.S. Holocaust Memorial Museum in Washington, D.C., and at a cemetery in Mobile, Alabama.[109]

Each of the class actions included claims for nuisance and unjust enrichment, and each sought disgorgement of profits or other monetary relief, and an injunction.[110] In September 2016, the Northern District of California consolidated the three lawsuits.[111]

The company responded that the app requires players to agree not to trespass. Before a person may play the game, he or she must agree to terms of service that instruct users not to "trespass, or in any manner attempt to gain access to any property or location where you do not have a right or permission to be." Niantic also argued that placing virtual objects on a virtual map did not qualify as an "unauthorized entry" into private property. The company also took the position that it is not responsible for the actions of third parties it does not control.[112]

After about one year of litigation, the court initially threw out the claims, citing the complaint's failure to explain the alleged damages, which is needed for the federal court to have jurisdiction over the claim.[113] The court's July 2017 ruling also found that the lawsuit defined the class so broadly that it could include anyone who owns or is near property, and that the governing law is unclear.[114] In response to the court's invitation to "more finely tune" the lawsuit,[115] however, the plaintiffs filed an

> *Trespass is a strict liability tort that arises when a person intentionally enters someone else's land without authorization or causes a 'thing' to do so. A virtual intrusion by a mythical creature will not suffice.*

amended complaint, alleging nuisance and trespass claims.[116] In response, the district court ruled in March 2018 that the proposed nationwide class action could proceed. U.S. District Judge James Donato found that since there are no definitive high court rulings on whether placing virtual objects on or near private property can trigger a viable trespass claim, "novel and open issues cut strongly against dismissal."[117]

Of course, these lawsuits do not allege ordinary trespass claims. Trespass is a strict liability tort that arises when a person intentionally enters someone else's land without authorization or causes a "thing" to do so.[118] A virtual intrusion by a mythical creature will not suffice. The Restatement (Second) of Torts does recognize, however, that intentionally causing a third party to enter land can constitute a trespass.[119] The question the federal district court in California and others will need to consider is whether an AR game or other application that merely encourages entry is sufficient to create liability or whether liability requires instructing someone to enter without permission or knowing they would do so.[120] For example, a Pokémon player could simply ask a homeowner whether he or she may enter a backyard, as occurred in the New Jersey case.[121]

While homeowners may have claims against individuals who actually enter their property without permission while playing the game, it is unsound policy to impose strict liability on a business that provides a product or service, reasonably assuming that users will ask permission before entering someone else's property (especially when they have agreed to do so). Imposing this type of liability would also disregard that some people welcome activities that draw people to their

> *While homeowners may have claims against individuals who actually enter their property without permission while playing the game, it is unsound policy to impose strict liability on a business that provides a product or service, reasonably assuming that users will ask permission before entering someone else's property.*

> *"Continuous automobile honking, glaring lights, loud music late at night, drunken parties, and disorderly conduct in a previously quiet residential neighborhood, resulting in scores of police calls, may support a nuisance claim. On the other hand, even a large number of distracted, enthusiastic gamers who visit and park their cars while searching for Pokémon does not rise to this level of actionable harm."*

neighborhood or property, whether they are PokéStops, concerts, sporting events, or a farmers' market. Such traffic may support local businesses, create a more vibrant community, and lead to positive interactions with visitors. While those who participate may occasionally cross private property, the sponsors of these activities have not committed a trespass and the law should not assume the worst in people. As Berkeley Law Professor Molly Shaffer Van Houweling has written, "Liability for tempting trespass should not chill products designed to suggest sociability."[122]

Nuisance claims against AR makers face similar challenges. A private nuisance is "a nontrespassory invasion of another's interest in the private use and enjoyment of land."[123] Not every interference with a plaintiff's use and enjoyment of land, however, supports a cause of action for nuisance. The conduct must be unreasonable,[124] considering such factors as the gravity of the claimed harm and the social value of the conduct.[125]

The standard for a viable nuisance claim is typically very high, otherwise there would be frequent lawsuits among neighbors. In Maryland, for example, to succeed on a nuisance claim, a plaintiff must establish "an unreasonable and substantial interference with his or her use and enjoyment of his or her property, such that the injury is of such a character as to diminish materially the value of the property as a dwelling and seriously interfere with the ordinary comfort and enjoyment of it."[126] Minor or even significant inconveniences do not give rise to a lawsuit.[127] Continuous automobile honking, glaring lights, loud music late at night, drunken parties, and disorderly conduct in a previously quiet residential neighborhood, resulting in scores of police calls, may support a nuisance claim.[128] On the other hand, even a large number of distracted, enthusiastic gamers who visit and park their cars while searching for Pokémon does not rise to this level of actionable harm.

> *As people become more immersed in VR games, not just controlling characters with a joystick or control pad but actually acting out and performing violent acts themselves (or via an avatar), plaintiffs' lawyers may encourage courts to revisit precedent.*

WILL VIRTUAL REALITY TECHNOLOGY SPARK A RESURGENCE OF LAWSUITS ALLEGING VIDEO GAME AND MOVIE MAKERS ARE RESPONSIBLE FOR VIOLENT ACTS?

There have long been claims that violence in video games may desensitize young people and inspire real attacks. Courts have dismissed such lawsuits against video game makers, given the limited liability for the criminal acts of third parties discussed above and because these types of claims raise First Amendment concerns regarding regulating the content of speech.[129] Product liability claims have also been dismissed because images and words in video games and movies do not qualify as "products" that are subject to traditional product liability law.[130]

As people become more immersed in VR games, not just controlling characters with a joystick or control pad but actually acting out and performing violent acts themselves (or via an avatar), plaintiffs' lawyers may encourage courts to revisit precedent. They may emphasize the deterrent role of tort law and urge courts to find liability. Such lawsuits would also provide an opportunity for advocacy groups that are frustrated with legislative inaction to address gun violence to attempt to regulate through litigation.

Virtual Theft and Violence, and Augmented Intrusions?

In the future, courts may be asked to address novel questions of whether virtual acts can lead to real tort claims or even crimes.[131]

In virtual reality environments, users will interact with others who are not physically present but share a virtual world. There may be instances where a person is "robbed" of an item that has monetary value during a virtual reality game. A person may be groped or stabbed in a VR game. The attack may seem real and cause real-life emotional trauma or even physical harm, such as a heart attack.[132] In an AR environment, a participant might cover another person's home, business, or

> *In the future, courts may be asked to address novel questions of whether virtual acts can lead to real tort claims or even crimes.*

church in racist messages or other offensive virtual graffiti.[133] Courts may be asked to decide whether conduct that occurs in a virtual or augmented reality setting can give rise to claims for intentional or negligent infliction of emotional distress, assault, battery, wrongful death, or violations of property rights.

These types of lawsuits may raise novel questions of jurisdiction, since those who engage in torts in a virtual environment, if they can be identified, can be physically located any place in the world.[134]

One entity that can be found and sued is the device maker or app provider. In some circumstances, these entities may be exposed to liability for the conduct of users. For example, a plaintiff might claim that an AR or VR provider acted negligently by creating a space that exposes visitors to a reasonably foreseeable harm that it could have prevented by incorporating a safeguard in the software or a mechanism for users to avoid an unwelcome or potentially harmful experience. Existing principles of law, applied to this new virtual context, should provide answers to most of these questions.

Virtual Employment Law

Using VR technology to bring employees in diverse locations together can create a more collaborative, personal, and productive environment. As businesses begin to use VR technology for meetings, training, and other purposes, they will need to consider establishing clear guidance for appropriate virtual workplace behavior. Companies will need to address basic questions, such as appropriate virtual workplace attire. In the virtual workplace, employers will also need to carefully monitor the same behaviors that can result in sexual harassment or employment discrimination claims in a physical workplace. Supervisors, employees, and others who participate in a virtual workplace will need to be educated that just because they are acting through an avatar, they are not excused from the standards of conduct that apply in real life.[135]

Privacy Concerns

As with any connected device that records and shares user data, VR and AR devices and apps raise privacy concerns. These concerns are elevated in situations where the technology tracks particularly sensitive information, like a user's hand, eye, and other physical movements and his or her

“Courts may be asked to decide whether conduct that occurs in a virtual or augmented reality setting can give rise to claims for intentional or negligent infliction of emotional distress, assault, battery, wrongful death, or violations of property rights.”

> *"Time-tested principles governing negligence, product liability, trespass, and nuisance that developed in the 'real world' apply regardless of whether someone was wearing a headset or peering into a smartphone … There appears to be no need for a new body of 'virtual tort law.'"*

location, and when the device may also gather information from children.

These types of concerns have been raised on Capitol Hill. In mid-2016, Al Franken, then the ranking Democrat on the Senate Judiciary Subcommittee on Privacy, Technology, and the Law, sent letters first to Oculus[136] and then to Niantic[137] asking questions about the data their technology gathers and shares. In response, Oculus explained why gathering information on physical movement is needed to make the technology work and improve the user's experience. Oculus also noted its privacy protections and explained that it strips recorded data of identifiable information, which seemed to satisfy Franken's concerns.[138] Niantic provided a similar response, also noting that it had "no plans to sell 'Pokémon Go' user data—aggregated, de-identified or otherwise—to any third party," but that it would provide reports with the number of visits players made to a location to retail partners that sponsor the game.[139] The company also updated the app to scale back its integration with users' Google accounts.

Other members of Congress continue to monitor these issues. In May 2017, a bipartisan group of legislators established a Congressional Caucus on Virtual, Augmented, and Mixed Reality Technologies, with the goal to educate their peers on the technology and to "encourage—rather than hinder—these enterprising fields."[140]

The Path Forward

While novel situations may arise, in most cases, lawsuits stemming from virtual and augmented reality technology fit within the existing framework provided by tort law. Time-tested principles governing negligence, product liability, trespass, and nuisance that developed in the "real world" apply regardless of whether someone was wearing a headset or peering into a smartphone. Tort law governing injuries from distracted driving or the criminal acts of third parties, for example, should apply equally in situations involving VR and AR devices or apps. Consistent with existing law, businesses that offer this technology will need to continue to educate consumers on how to safely use it by providing adequate instructions, warnings, information on gathering and sharing data, and other safeguards. There appears to be no need for a new body of "virtual tort law."

Wearable Devices

Wearable devices can be worn on the body as bracelets or watches, or even incorporated into a user's clothing. They can then seamlessly track every part of the user's day, including location, activity level, heart rate, food intake, and sleep, and stream this biometric data directly back to the user's smartphone or computer in real time, often while storing the data in the cloud. They are analogous to airplanes' "black box" recorders, keeping track of the user's health and activities during every moment the user is wearing them. The amount and type of data they collect and store raise privacy and data security concerns. In addition, the material collected may become important discoverable information in future litigation.

Wearable technology, such as smart watches and fitness trackers, along with mobile medical apps, have already become an integral part of many people's daily lives. With advancements in processing speeds, data storage, and connectivity, manufacturers have developed these products to meet the demand of an increasingly tech-savvy and health-conscious population. Technology that was once limited to medical offices, gym treadmills, and other aerobic exercise machines can now be worn on a user's wrist or carried in a pocket.

> *"[O]ver 78,000 new medical apps were added to the major app stores last year, and an estimated 3.6 million medical apps were downloaded in 2017."*

The wearable device market is already generating billions in revenue, and the market for these new products continues to grow.[141] Last year, an estimated 113.2 million wearable devices were shipped worldwide, and annual shipments are projected to increase to 222.3 million by 2021.[142] In addition, over 78,000 new medical apps were added to the major app stores last year, and an estimated 3.6 million medical apps were downloaded in 2017.[143] There are currently over 325,000 medical apps available for download, and investors continue to funnel billions of dollars into developing more of them.[144]

Medical apps generally work by utilizing the user's smartphone. The app uses the built-in features of the smartphone, which allow it to track data the phone gathers, such as location and movement, as well as information the user enters, such as food intake. Since medical apps are generally installed on the user's smartphone and often run in the background—and since smartphones are always with us, and always on—they can collect a wide variety and vast amount of the user's information. They can then present the user's information in a dashboard or diagnosis-like format. Available medical apps support diet and exercise programs and provide pregnancy trackers, symptom checkers, sleep and relaxation aids, and self-diagnostic tools.

Wearables are networked devices that generally attach to the user's body as a bracelet or watch. They can also be incorporated into the user's clothing or worn as glasses. These products utilize sensors to collect and track a broad range of biometric data, including heart rate, activity level, skin temperature, respiratory rate, and the number of daily steps the user takes, as well the user's geographic location. The device tracks and stores this information while the user wears it throughout the day and even while he or she sleeps. The data are then collected and transferred to the user's smartphone, personal computer, cloud service, and/or social network. With these devices, users can view a more complete picture of their health.

> *"Self-monitoring, tracking, and sharing with friends and family the data collected by these products can provide significant health benefits."*

Fitbit is an example of one of the more popular wearable fitness trackers on the market. Fitbit is a bracelet worn on the user's wrist that can record the number of steps taken, pace, elevation, stairs climbed, distance traveled, active minutes, stationary time, breathing patterns, continuous heart rate, calories burned, sleeping patterns, and precise location.[145] The device then connects to an app that allows users to track their daily activity and measure their progress toward their fitness goals. It also allows users to connect with friends and share results via email or Facebook.[146]

Self-monitoring, tracking, and sharing the data collected by these products with friends and family can provide significant health benefits. According to one poll, 82 percent of users said these products

enhanced their lives.[147] Users who choose the option to share their data with friends and family may become more motivated to reach their fitness goals.[148] In addition, because users can more closely track their daily movement and vitals, they can more effectively self-monitor their own health and identify potential issues. Stories about how these products have provided life-saving alerts to users have become increasingly common. For example, an Apple Watch user sought immediate medical attention after he noticed a spike in his resting heart rate, and during his examination, doctors discovered that the spike was due to a life-threatening blood clot in his lungs.[149] Another user of an Apple Watch discovered that she had an overactive thyroid after seeking medical attention when she noticed her heart rate never slowed down.[150] Her doctors explained that without treatment, she was at an increased risk of a heart attack. It is estimated that wearable devices could save up to 1.3 million lives by 2020.[151]

Given the health benefits of these products, employers are encouraging their employees to use them and to share their fitness data. In exchange for sharing this information, employers often provide these products at a discount or free as part of their corporate wellness programs, in an effort to improve their employees' health and lower company healthcare costs. For example, Appirio received a $300,000 discount on its $5 million insurance premiums by sharing employee health data with its insurer and showing that its employees' health was improving.[152] British Petroleum (BP) employees were eligible for a discount if they reached their step goals during the company's Million Step Challenge through Fitbit.[153] BP also provided free Fitbits to employees and a chance to lower their insurance bills by $1,200 in exchange for wearing the device and logging a sufficient amount of physical activity.[154]

Insurance companies are also encouraging individual policyholders to use such devices. For example, in 2015, John Hancock began offering insurance advantages to individuals who agreed to provide their fitness and activity data.[155] The program allows policyholders to earn discounts, gift cards, and discounted hotel stays and airline fares in exchange for points earned through physical activity and doctor visits.[156]

In addition to collecting biometric information in order to implement health and wellness plans, companies are collecting such biometric information as fingerprints; voiceprints; and scans of hands, retinas, and facial geometry. With new and more readily available technology, companies are discovering the benefits of employing biometric-based tools. For example, companies are switching from traditional to biometric time clocks, which

> *"Given the amount of health-related biometric information being collected, along with the dangers of self-diagnoses, the manufacturers face legal and regulatory risks."*

allow employees to clock in and out with a fingerprint or other biometric ID rather than a time card. Since time cards can be lost or stolen, biometric clocks help eliminate time theft and ensure more accurate compliance with attendance policies. Companies are also using finger and palm print readers, as well as iris and retina scanners, to secure their facilities and verify transactions. Every day, people unlock their smartphones with their fingerprint and those using the newest iPhone can unlock it with facial recognition.

Given the amount of health-related biometric information being collected, along with the dangers of self-diagnoses, the manufacturers face legal and regulatory risks. Manufacturers must consider the liability risks associated with marketing and distributing wearable devices and medical apps that may not perform as intended or advertised. In addition, the information these products collect will increasingly be used as evidence in litigation. Location, movement, and health data from these devices may be sought in discovery, as they could be used to dispute any claim related to personal injury or workers' compensation, or as evidence in a criminal trial. Finally, companies that collect, store, utilize, or share biometric information with third parties must consider privacy rights and data security requirements.

The Regulatory Landscape

Wearable devices and medical apps face a complicated regulatory landscape governed by federal agencies including the FDA, FTC, and the Department of Health and Human Services Office for Civil Rights (OCR).

FDA GUIDANCE ON MOBILE MEDICAL APPLICATIONS AND WELLNESS DEVICES

The FDA, which is primarily focused on protecting patient safety, has issued guidance to developers of mobile medical apps.[157] Through this guidance, the FDA seeks to strike a balance by providing a risk-based approach and focusing its oversight on the subset of medical apps that present the greatest risk to patients if they do not work as intended. Those identified medical apps are required to follow the traditional FDA controls on medical devices.[158]

For those medical apps that meet the definition of a medical device under section 201(h) of the Food, Drug, and Cosmetic Act[159] but present a lower risk to patient safety, the FDA has announced that it will exercise "enforcement discretion." The guidance provides examples of such medical apps, including those that (1) facilitate supplemental clinical care by coaching patients to manage their health in their daily environment, (2) provide simple tools for users to organize and track their health information, and (3) provide easy access to information related to users' health conditions or treatments.

> *In 2016, the FDA issued guidance indicating that it did not intend to regulate low-risk general wellness devices.*

In 2016, the FDA issued guidance indicating that it did not intend to regulate low-risk general wellness devices.[160] "General wellness" products fall into two categories. The first covers products that their makers claim can sustain or encourage a general state of health, without referencing specific diseases or conditions. These general wellness claims can relate to weight management, physical fitness, relaxation or stress management, and sleep management. The FDA provides a list of general wellness claims that fit this category, including claims to (1) promote or maintain a healthy weight or encourage healthy eating; (2) promote relaxation or manage stress; (3) promote physical fitness, by helping users log, track, or trend exercise activity, measure aerobic fitness, improve physical fitness, or improve energy; (4) promote sleep management; and (5) enhance participation in recreational activities by monitoring the consequences of participating in such activities.

The second category of general wellness products covers those making claims that users can sustain or encourage a general state of health, with reference to specific diseases or conditions. These claims may suggest that the medical app may, as part of a healthy lifestyle, help reduce the risk of certain chronic diseases or conditions or may increase the quality of life of users living with certain chronic diseases or conditions. For example, a medical app that tracks and records sleep, work, and exercise routines may claim that, as part of a healthy lifestyle, it may help one live better with anxiety, or a medical app that promotes physical activity may claim that, as a part of a healthy lifestyle, it may help reduce the risk of high blood pressure.

Since the FDA has decided to exercise enforcement discretion with these lower-risk medical apps and general wellness devices, businesses that create these products will not be required to apply to the FDA for premarket approval or to engage in post-market reporting. Since these apps fall outside the FDA's enforcement purview, however, product liability litigation associated with their use will not be preempted by federal law. Manufacturers of these devices also face other liability risks, such as claims that allege the products are marketed in a misleading way or that assert a breach of express or implied warranties related to the product's performance.

FTC ENFORCEMENT AND REGULATION OF WEARABLE DEVICES AND MEDICAL APPS

The FTC is charged with protecting consumers from deceptive and unfair trade practices (as are state consumer protection agencies and state attorneys general with consumer protection authority). The FTC has two major concerns with wearable devices and medical apps: how they are marketed and how they protect consumer data and privacy.

To advise developers, the FTC has developed guidance documents, including a "Best Practices" overview for medical app

developers.[161] In January 2015, the FTC released a detailed report, "Internet of Things: Privacy & Security in a Connected World."[162] The report urges product designers and manufacturers to adopt best practices, such as putting a strong focus on data security and upholding consumer expectations. The FTC has also created a web-based tool that is designed to help developers understand what federal laws and regulations might apply to their medical apps.[163] The FTC developed this tool in conjunction with the FDA, OCR, and the Office of the National Coordinator for Health Information Technology.[164]

The FTC has expressed concern regarding the growing use of wearable devices and medical apps and the lack of privacy laws governing them. In 2014, the FTC reported the results of a study that tracked data transmissions from 12 mobile apps and two wearable devices. For the 12 mobile apps it tested, it found that user information ranging from device information, gender, and diet information was sent to 76 third parties by the app or its vendor. One app it tested sent information to 18 different third parties.[165]

The FTC is increasing its level of activity regarding data privacy. It has targeted companies that fail to disclose to users that their personal data are collected without consent.[166] In one particular action, the FTC pursued a flashlight app that was collecting user location data without disclosure to consumers.[167] The FTC has also brought enforcement actions against developers that it believes have failed to install sufficient security controls.[168]

The FTC is also using its authority to go after medical apps that it views as making unsubstantiated or misleading claims. The agency took its first action in the medical app marketplace against the makers of AcneApp and Acne Pwner,[169] both of which purported to treat acne with colored lights emitted from smartphones or mobile devices. The consent order barred the apps' marketers from claiming light could treat acne. In addition, the FTC took an enforcement action against MelApp and Mole Detective. These medical apps claimed to increase consumers' chances of detecting melanoma by analyzing pictures of their moles and skin lesions.[170] Marketers for both apps agreed to settlements. The marketer for MelApp agreed to a $17,063 fine as part of the settlement, and the marketer of Mole Detective agreed to a $3,930 fine.[171]

In addition to the FTC, state attorneys general are taking action over data privacy concerns under state consumer protection laws. For example, in 2012, California's attorney general reached an agreement with six companies, including Apple, Google, HP, and Amazon, to strengthen privacy protections for users of medical apps.[172]

"The FTC has expressed concern regarding the growing use of wearable devices and medical apps and the lack of privacy laws governing them."

PRIVACY AND THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

The Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects the confidentiality of patients' health information. HIPAA generally prohibits unauthorized disclosures of protected health information except for a legitimate medical, business, or public health use as defined in the statute and regulations. To be covered under the HIPAA privacy rule, however, the information must be personally identifiable and held by "covered entities." Covered entities include health insurance plans, healthcare clearinghouses, and healthcare providers. The HIPAA privacy rule can also cover "business associates" that covered entities hire to help them carry out healthcare functions. HIPAA does not create a private cause of action. Only the OCR may investigate and impose civil and criminal penalties against a healthcare provider for HIPAA violations.

It is unlikely that manufacturers and developers of wearable fitness-type devices and apps will be subject to HIPAA's requirements as they do not qualify as covered entities. Even the collection of health data by a covered entity such as a health insurer may fall outside the scope of HIPAA when the information is not personally identifiable.

STATE BIOMETRIC PRIVACY LAWS AND THE COLLECTION OF BIOMETRIC DATA

Biometrics is simply the measurement of a person's physical being. Wearables and medical apps collect behavioral characteristics (e.g., steps taken per day) and physiological characteristics (e.g., heart rate). A few states, including Illinois,[173] Texas,[174] and Washington,[175] have enacted legislation specifically to regulate the use and collection of an individual's biometric information.

The Illinois Biometric Information Privacy Act (BIPA) is one of the most stringent state laws on consent, notice, and disclosure procedures for biometric info. BIPA regulates the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information,[176] and it applies to all private entities, which are defined as any "individual, partnership, corporation, limited liability company, association, or other group, however organized."[177]

BIPA defines a biometric identifier to include "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[178] Specifically exempted from the definition of "biometric identifier" are photographs of an individual, writing samples, demographic data, and physical descriptions. Likewise, biometric information is broadly defined to include "any information, regardless of how it is

"The Illinois Biometric Information Privacy Act (BIPA) is one of the most stringent state laws on consent, notice, and disclosure procedures for biometric information."

captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual,"[179] and has similar exclusions.[180]

Although photographs are excluded from the definition of "biometric identifier," courts have interpreted the "scan of … face geometry" under the biometric identifier definition to include measurements derived from photographs.[181] One court stated that "'[p]hotographs' is better understood to mean paper prints of photographs, not digitized images stored as a computer file and uploaded to the Internet."[182] Thus, the use of facial recognition software to identify an individual on stored digital photographs can violate BIPA.[183]

BIPA requires any private entity that collects or obtains biometric identifiers or information to (1) inform the individual in writing that a biometric identifier is being collected or stored; (2) inform the individual in writing of the specific purpose and length of time for which the biometric identifier is being collected, stored, and used; and (3) receive a written release executed by the individual assenting to the collection, storage, and use of a biometric identifier.[184] Absent a court order or law enforcement directive, a private entity may not share biometric information without express consent from the individual. Additionally, a private entity may not sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifiers or information.

Significantly, BIPA allows individuals to bring private lawsuits to enforce its provisions.[185] The Illinois statute is the only state biometric privacy law that includes a private right of action. BIPA allows plaintiffs to seek actual damages or statutory damages of $1,000 for each negligent violation and $5,000 for each willful or reckless violation.[186] BIPA also provides that a prevailing party may recover attorneys' fees, expert witness fees, and litigation costs and expenses. Biometric privacy laws adopted by Texas and Washington, unlike Illinois, require enforcement actions to be filed by the state attorney general.[187]

"The Illinois statute is the only state biometric privacy law that includes a private right of action."

It is unclear if private entities will face liability for mere statutory violations of BIPA or if plaintiffs will need to show actual injury in order to recover statutory damages, but some recent court decisions suggest that plaintiffs will need to allege an actual injury. These courts have read the term "aggrieved" under Section 20 of BIPA, which states that "[a]ny person aggrieved by a violation of this Act shall have a right of action," to require an actual injury. For example, in *McCollough v. Smarte Carte, Inc.*, the U.S. District Court for the Northern District of Illinois held that "by limiting the right to sue to persons aggrieved by a violation of the act, the Illinois legislature intended to include only persons having suffered an injury from a violation as 'aggrieved.'"[188] In addition, an Illinois appellate court weighed in on BIPA for the

first time in *Rosenbach v. Six Flags Entertainment Corp*. The court held that in cases where "a person alleges only a technical violation of the Act without alleging any injury or adverse effect, then he or she is not aggrieved and may not recover under any of the provisions in section 20."[189]

These decisions have the potential to foreclose BIPA class actions that allege only a technical violation of BIPA without an underlying injury. However, *Rosenbach* is the first and only Illinois appellate court to interpret BIPA, and the Illinois Supreme Court has not yet weighed in. It is unclear whether courts will follow the *Rosenbach* decision, and with the number of filed BIPA class actions that allege only a technical violation, litigation on this subject will likely continue.

The application of BIPA to any private entity as well as its broad definition of "biometric identifier and information" has created enormous liability risks.[190] This risk would be further expanded if the Illinois Supreme Court decides that all a plaintiff must allege is a technical violation of the statute in order to recover statutory penalties. Due to BIPA's wide scope and the opportunity to obtain statutory penalties, the plaintiffs' class action bar has taken notice of it and has filed over 60 class actions in recent years.[191]

While wearable devices and medical apps have not yet been targeted by plaintiffs' attorneys under this law, businesses such as video game companies, airlines, nursing homes, hotel chains, food product manufacturers, gas stations, and restaurant chains as well as online platforms like Facebook and Google have had actions filed against them under BIPA.[192] Courts have dismissed a few of these actions at the pleading stage, but most are ongoing. One settled for $1.5 million.[193]

With the potential liability exposure created by BIPA, some companies are refusing to offer their products in Illinois. For example, Google refused to release in Illinois the portrait-matching feature in its popular Google Arts & Culture app.[194] The app uses facial recognition and compares the image of the user with thousands of famous portraits housed in its database. The app then presents the user with matches of his or her artistic doppelganger. In addition, Nest, a company that specializes in thermostats and home security systems, will not provide one of its security systems in Illinois because its doorbell camera uses facial recognition.[195]

"Due to BIPA's wide scope and the opportunity to obtain statutory penalties, the plaintiffs' class action bar has taken notice of it and has filed over 60 class actions in recent years."

Exposure to Product Liability and Consumer Litigation

Manufacturers of wearable devices and medical apps also face exposure to state tort and consumer protection claims brought by or on behalf of device users.

Hundreds of thousands of people already visit the emergency room for injuries related to exercise equipment.[196] Since wearable devices and medical apps are often designed to supplement and help people with their fitness goals, manufacturers are likely to see claims alleging that their products either created a distraction or directly caused these injuries.

For example, in 2012, the family of a cyclist who died in an accident brought an action against a bicycling app that awarded a "King of the Mountain" status to top performers. The family argued that the cyclist would not have had the accident if he was not trying to regain his top performer status on such a dangerous road. The developers of the app, the lawsuit said, should have known the app would encourage such risk taking, yet they failed to warn that the road conditions were not suitable for such racing.[197] The judge dismissed the claim, finding that the cyclist assumed the risks of bicycling and that the defendant had shown that bicycling is an inherently risky activity.[198]

While product liability and other personal injury claims against medical app makers are rare, firms are advertising for future plaintiffs to bring such lawsuits.

> *"Location, movement, and health data from these devices may provide valuable discoverable information in many types of litigation."*

A growing area of litigation is consumer fraud and false advertising claims involving regulated products.[199] Manufacturers of wearable devices and medical apps are a likely target for such claims by plaintiffs' lawyers. For example, Fitbit, Inc., has already been hit with two such class actions in California. The first complaint alleges that Fitbit misled consumers about the accuracy and reliability of its sleep-tracking function. The complaint states that the Fitbit sleep-tracking devices "consistently misidentify" sleep and may overestimate sleep by as much as 67 minutes.[200] This case is still in active litigation. The second complaint, filed in 2016, similarly alleges that Fitbit misled consumers about the accuracy and reliability of its heart rate monitoring function.[201] This case was recently moved to arbitration.[202]

Impact on Discovery and Litigation

Location, movement, and health data from wearable devices may provide valuable discoverable information in many types of litigation. Tracking data from a fitness device could be used to provide an alibi in a criminal case. Fitness data could also be used to cast doubts on the alleged injuries in an insurance claim or personal injury lawsuit. In employment cases, the data could assist in evaluating workplace injuries or disability claims.

Canadian courts have already seen data from a Fitbit used in two disability cases and a personal injury case. In the two separate disability cases, petitioners used Fitbit data to support their claims of insomnia. In a personal injury case, a woman used her Fitbit data to support her claim that her physical activity was affected following a car accident.[203]

In Pennsylvania, police have used data from a Fitbit to support charging a person with filing a false report with law enforcement, creating a false alarm to public safety, and tampering with evidence.[204] In that case, police called to the defendant's home found a knife, a bottle of vodka, and furniture in disarray. The defendant claimed she was woken up and sexually assaulted by a man. Evidence from the defendant's Fitbit contradicted these statements. During the time that she alleged that she was sleeping, her Fitbit indicated that she was awake, alert, and walking around. The prosecution used this evidence to support its claim that she staged a fake crime scene during this period. The defendant pled guilty and had to complete two years of probation.

Evidence from a Fitbit has also led to a murder arrest in Connecticut. There, a husband became a prime suspect in his wife's murder due to discrepancies in his alibi. Police examined his wife's Fitbit and discovered that she had logged numerous steps after the time the husband claimed she was killed.[205] The combination of the Fitbit data and additional circumstantial evidence led to the husband's arrest for murder, tampering with evidence, and providing a false statement. Data from this Fitbit will also likely be used in the wrongful death action filed by the deceased woman's sister against the husband.

Although the information recorded by these devices could prove useful in all types of litigation, there currently are relatively few examples of how courts will handle disputes involving the discovery of such data.

An initial question to consider when seeking such data is who actually owns the information—the user or the device's manufacturer? Additionally, attorneys must consider the device's privacy policy. For example, Fitbit will share a user's data when the user authorizes Fitbit to share it.[206] In cases where the user's consent cannot be obtained, Fitbit has agreed to provide the data "to comply with a law, regulation, legal process, or governmental request; to assert legal rights or defend against legal claims; or to prevent, detect, or investigate illegal activity, fraud, abuse, violations of our terms, or threats to the security of the Services or the physical safety of any person."[207] In cases where the user refuses to provide consent, a court order or subpoena will most likely be necessary to obtain the data. It is unclear what challenges may arise if a party asks

the court to serve a subpoena on a device manufacturer. When deciding whether to grant such a motion, the court will likely balance whether the person has a reasonable expectation of privacy against the probative value of the information and how prejudicial it may be to the non-requesting party.

Another issue is whether and to what extent the data are admissible at trial. As with any admissible evidence, the information must be relevant. Relevant evidence is evidence that has any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence. In cases where a person's health or location at a given time is at issue, this seems to be a fairly straightforward question. Of course, opponents to admission of this evidence will raise objections, including hearsay, authentication concerns, and reliability issues.

A Wisconsin state court recently went through this type of analysis after the state tried to enter into evidence location and sleep data from a Fitbit that refuted a defendant's story about the Fitbit's user being present at the scene of the crime.[208] Attorneys for the defendant attacked the reliability and authenticity of the Fitbit data and argued that the evidence was hearsay. The court first dealt with the reliability issue, denying admission of the sleep data because their reliability and accuracy were being litigated in a consumer class action. The court admitted the step-counting data since no such reliability claims had been made against them. It also reasoned that the defendant could question the Fitbit user about the data's reliability and present his own expert witness on the subject. The court then found that the Fitbit data were computer-generated records and thus not hearsay. Even if the data were hearsay, the court found they fell within the "Records of Regularly Conducted Activity" exception to the rule. The court concluded by finding that the record was self-authenticating since it was a record of regularly conducted activity, and that an affidavit provided by a Fitbit official sufficiently authenticated it.

To avoid some of these objections and get such data admitted, one commentator suggested having a qualified expert review the data pulled from the wearable and use this information as the basis of his or her opinion, as an expert can rely on evidence that is not admissible at trial.[209] The expert could then testify that he or she relied on the data, and the jury could determine their reliability and weight as evidence. An opposing party may object to this testimony, however, on the ground that a reasonable expert should not rely on such evidence in forming his or her opinions.

The Path Forward

The wearable device and medical app industry is thriving. It is providing people with an opportunity to take more control over their healthcare while motivating people to become healthier. The industry is growing rapidly, in part because the federal government and most states have taken a balanced approach to regulatory and liability issues.

Given the enormous amount of biometric information being collected, stored, utilized, and shared, there are legitimate privacy concerns. The explosion of litigation under Illinois' BIPA, however, should give state legislatures pause in considering new laws on the subject. Any future laws that regulate biometric information should be narrowly tailored to specific types and problematic uses of biometric information, and should not include a broad new private right of action.

"The explosion of litigation under Illinois' BIPA, however, should give state legislatures pause in considering new laws on the subject."

3D Printing

3D printing will continue to disrupt traditional manufacturing and may lead to a new industrial revolution.[210] While this technology has been available to manufacturers since the 1980s, 3D printers recently exploded onto other markets, such as hospitals and apparel, and personal versions are now found in homes as well.[211] As ordinary people and businesses that do not traditionally make products become manufacturers, 3D printing is poised to have a significant effect on tort law.

3D printing, also known as additive manufacturing, uses a machine to turn digital blueprints into physical objects.[212] Blueprints come in the form of computer-aided designs (CADs) that provide virtual 3D models of the item that will be created. Individuals can create CADs and upload them to the internet for others to use for free or to purchase. CADs can also be commissioned. For example, a doctor could send a CT scan of a patient's knee to a designer who can then develop a customized CAD for an artificial knee. A 3D printer can then print the CAD for implant via knee replacement surgery.[213]

3D printing is often welcomed as an efficient, cost-effective, and waste-reducing means of manufacturing products or component parts. Unlike traditional manufacturing, where the process begins with a block of material that is reshaped into the desired form, 3D printing works in reverse, starting from scratch and adding only the materials necessary to create the final product.[214] By manufacturing with 3D technology, a final product can be created as one integrated piece with internal, movable parts since products are created one layer at a time.

3D printers are also different from mass manufacturing in that products can be customized for a single consumer. Traditional manufacturers make the same standardized product to put on the market, but 3D printing allows products to be tailored to meet an individual's specific needs, tastes, and measurements.[215] 3D printing is making unparalleled advancements in industries including healthcare, automobiles, aerospace, food, fashion, and the military.[216]

Hobbyists can also buy 3D printers from most major online tech retailers or local tech stores, starting at just under three hundred dollars.[217] Major manufacturers might spend up to $2.5 million for state-of-the-art 3D printing technology.[218] The market for 3D printing is rapidly expanding with the technology's capabilities and applications. Some 97 manufacturers produced and sold 3D printing systems in 2016, up from 62 in 2015 and 49 in 2014.[219] The 3D printing industry reached just over $6 billion in revenues in 2016.[220] In a survey of almost a thousand individual consumers in the 3D printing market, results showed that of those using 3D printers, 44 percent were professionals, 47 percent were hobbyists, and nine percent identified as "other."[221] Of companies using 3D technology, the reason cited most often for doing so is to accelerate product development, followed by the ability to offer customized products and limited series items.[222]

As 3D printers become more affordable, their presence will expand and level manufacturing itself, allowing anyone who owns a 3D printer to assume the mantle of "manufacturer."[223] Eventually, having a "CAD file of an object, such as a coffee cup or a toy, will essentially be the equivalent of having the physical object—it is just a click away."[224] There is virtually no legal precedent associated with 3D printing. As this revolution occurs and injuries associated with 3D-printed products or parts inevitably arise, courts will grapple with such basic questions as who is a manufacturer, what qualifies as a product, and who is legally responsible for any harm stemming from it?

3D Printing in Action

Imagine a day when an auto repair shop can 3D print a new car part on site, or a hospital can 3D print a new human organ from a patient's own cells. These possibilities will likely become reality sooner rather than later, so long as development of the technology is not deterred or delayed by excessive liability or government regulations beyond those reasonably necessary to protect public safety.

AUTOMOTIVE

Major auto companies are looking to 3D printing technology to more quickly respond to consumer demands. They are using 3D printing to accelerate product design and the quality of prototypes.[225] 3D printing technology also allows automakers to affordably customize vehicles and develop stronger, more efficient, lightweight designs. It can simplify both complex and small production, enabling manufacturers to print a single component on demand. One machine can support unlimited product lines.[226]

In 2017, Ford became the first major automaker to purchase a Stratasys Infinite

"As 3D printers become more affordable, their presence will expand and level manufacturing itself, allowing anyone who owns a 3D printer to assume the mantle of 'manufacturer.'"

3D Printer for future performance products and personalized auto parts.[227] Other companies, such as Volkswagen, are also moving into 3D printing.[228]

3D printing also has the potential to revolutionize the auto repair industry, making it easier to obtain spare parts. Daimler, for example, has begun using 3D printing to make plastic replacement parts and is moving into metal parts for older commercial Mercedes trucks.[229] Before long, local auto shops may be able to print parts for repairs. In fact, for years Jay Leno has relied on a sophisticated scanner and 3D printer to replace obsolete parts in his collection of antique cars.[230]

AEROSPACE

In the aerospace industry, General Electric's (GE's) move toward 3D printing technology began with a nozzle tip for planes that sprays fuel into a jet engine.[231] The 3D-printed nozzle tip "not only combined all 20 parts into a single unit, but it also weigh[s] 25 percent less than an ordinary nozzle and [is] more than five times as durable."[232] Getting to the heart of 3D printing benefits, GE explains that complexity in manufacturing is historically expensive, but with 3D printing, companies can achieve both sophistication and cost reduction at the same time.[233]

Following its success with the fuel nozzle, GE began to purchase 3D printing technology and, over an 18-month period, its research team was able to reduce 900 separate helicopter engine components to just 16 parts.[234] The 3D-printed parts were 40 percent lighter and 60 percent cheaper than the original parts.[235] GE's successful experiment led the company to significantly expand its investment in companies that make 3D printers. GE has used the technology to create prototypes for turboprop engines and turbine blades, and is looking to expand its involvement in 3D printing to other industries.[236] According to the company, it is now using over 300 3D printers and investing billions of dollars per year in the technology.[237]

"The FDA has reviewed over 100 medical devices currently on the market that were made with 3D printers..."

HEALTHCARE

Perhaps no industry has embraced or benefited more from advances in 3D printing technology than the healthcare industry.

The FDA has reviewed over 100 medical devices currently on the market that were made with 3D printers,[238] including orthopedic and cranial implants, surgical instruments, dental restorations, and prosthetics. Many of these products are customized to fit each patient. The FDA has also granted emergency exemptions for devices not yet approved. In 2012, the FDA granted an emergency exemption for the implant of a 3D-printed trachea into a six-week-old infant.[239] A year later, the FDA again granted an emergency exemption for a man to have 3D-printed plates replace 75 percent of his skull.[240]

Pharmaceutical companies are using 3D printing technology to develop medications.

In 2015, the FDA approved the first 3D-printed drug, Spritam, from Aprecia Pharmaceuticals. The 3D printing of Spritam allows the medication to dissolve in the mouth and be absorbed quickly, helping prevent or reduce the severity of an oncoming epileptic seizure.[241]

In addition, 3D printing technology known as "bioprinting" can "produce living tissue, bone, blood vessels, and potentially, whole organs for use in medical procedures, training and testing."[242] Bioprinted tissue may be a game changer for developing and testing how new drugs affect human cells.[243] Although bioprinting is in the early stages of development, it shows immense promise for medical treatment, with the end goal of 3D printing replacement organs.[244]

Many Liability Questions, Few Answers

Because 3D printing has the potential to make any person a manufacturer, courts will be faced with novel questions as to when and how product liability law applies when a plaintiff claims he or she was harmed by a 3D-printed product. Key questions include whether a CAD qualifies as a "product" and who qualifies as a "product seller." The answers to these questions will determine whether an individual or company is subject to product liability law or general negligence principles when an injury is associated with a 3D-printed product.

IS A COMPUTER-AIDED DESIGN A "PRODUCT"?

An emerging issue with respect to such liability is whether a person who develops a CAD has created a product.

The Restatement (Third) of Torts defines "product" as a "tangible personal property distributed commercially for use or consumption."[245] It is clear that a final 3D-printed object is a product. It is less certain whether CAD files are products, since they are basically electronic blueprints or instructions for creating products, not physical objects themselves.

Generally, courts do not consider purely electronic data, such as software or code, to be products.[246] Similarly, architectural blueprints and intangible content associated with products are not subject to product liability law.[247]

Courts have not specifically considered whether CAD files constitute electronic information, which falls outside product liability law. In addition, the "distributed commercially" requirement for product liability suggests that CADs, when not purchased but shared without charge or developed by the user, may not qualify as a product.

"Courts have not specifically considered whether CAD files constitute electronic information, which falls outside product liability law."

> *"[C]ourts may now be willing to stretch the definition of 'product' to include electronic files used to make bespoke 3D-printed objects..."*

Legal scholars observe, however, that "[c]ourts may now be willing to stretch the definition of 'product' to include electronic files used to make bespoke 3D-printed objects," reasoning that the file was part and parcel of the completed product.[248]

WHO IS A PRODUCT SELLER?

Even if courts find that CADs are "products," they will have to decide whether those who use 3D printing to make products or components are "product sellers" before subjecting them to product liability law.

The Restatement (Third) of Torts, Products Liability, provides that "[o]ne engaged in the business of selling or otherwise distributing products who sells or distributes a defective product is subject to liability for harm to persons or property caused by the defect."[249] A person who or business that fits this definition is subject to strict liability if a manufacturing flaw causes an injury. Product sellers are also subject to liability if the product's design is defective. When courts evaluate the liability of product sellers, they may consider whether there was a reasonable, feasible, safer alternative design that would have reduced the risk of injury or avoided the harm. Product sellers also have an obligation to provide users with instructions or warnings needed to avoid risks of injury.

The "business of selling" language in the definition of "product seller" limits these liability principles to those who regularly sell products and excludes those who make an occasional sale or give products as gifts.[250] In a world where 3D printing becomes commonplace, the line between a commercial seller and occasional seller may blur.[251]

WHO IS SUBJECT TO LIABILITY?

As the 3D printing industry grows, products will be made by nontraditional sources including hospitals, repair shops, and even consumers in their own homes; none of them would likely face product liability actions based on current definitions.[252] A 3D-printed product may be defective for many reasons, such as (1) it was printed based on a CAD for a defective product, (2) a computer glitch led to a flawed CAD when it was designed or while the file was downloading, (3) the 3D printer itself was defective and corrupted the product, (4) the raw material used in creating the product was defective, (5) human error occurred in creating the CAD, or (6) human error occurred in using the 3D printer.[253]

> *"In a world where 3D printing becomes commonplace, the line between a commercial seller and occasional seller may blur."*

> *For a plaintiffs' lawyer, the question becomes who should be named as a defendant and under what theories of liability?*

Imagine the 3D printing lifecycle of a coffee mug: Someone designs a CAD for the mug and uploads it to the internet, where people can freely access it. An individual finds the CAD but wants a different handle, so he or she modifies the CAD and puts it on a CAD-sharing website. Another individual downloads the modified CAD coffee mug and prints it at home for free. Alternatively, he or she could select the CAD design and pay to have the mug printed by another party and shipped to him or her already constructed. Then, the mug shatters when hot liquid is poured into it, causing serious burns.[254]

This simple hypothetical illustrates the potential room for error with no clear way to know where in the design and manufacturing process a potential defect occurred. For a plaintiffs' lawyer, the question becomes who should be named as a defendant and under what theories of liability? Lawyers will likely consider suing all of the entities in the supply chain. That could mean the manufacturers and sellers of 3D printers, the creators and sellers of CAD blueprint designs, the creators and sellers of the "ink" used for 3D printers, the manufacturers who use 3D printers to put products on the market, and the sellers of 3D-printed products.

IF PRODUCT LIABILITY LAW DOES NOT APPLY, THEN WHAT DOES?

Ordinary product liability law is likely to apply in cases involving traditional manufacturers that use 3D printing to construct products or component parts. The more difficult cases will involve 3D-printed products made by nontraditional manufacturers, such as hobbyists who make a toy, a hospital that prints a custom joint implant, an auto repair shop that prints a new bolt, or the plaintiff himself or herself. In these situations, plaintiffs are likely to rely heavily on common law negligence claims. While these types of claims require a showing of fault, they are flexible and subject to judicial expansions of liability, as shown below.

In the event of a product failure and injury, the general inquiry under negligence law is whether the defendant had a duty of reasonable care to the plaintiff, whether the defendant fulfilled this duty by addressing

> *The more difficult cases will involve 3D-printed products made by nontraditional manufacturers, such as hobbyists who make a toy, a hospital that prints a custom joint implant, an auto repair shop that prints a new bolt, or the plaintiff himself or herself.*

reasonably foreseeable risks of injury associated with the product, and whether a violation of the duty of care caused the plaintiff's injury.

In evaluating the liability of a nontraditional manufacturer, courts might consider whether that party obtained the CAD file from a reputable source (rather than a design that was anonymously uploaded or one that was "open sourced" and could have been dangerously modified or corrupted), appropriately maintained its 3D printer, and used the proper materials. CAD designers may also be on the hook, facing allegations that it was reasonably foreseeable that their designs would be downloaded and used to create dangerous products.

Traditional liability principles should place significant constraints on such liability. For example, a CAD designer's duty to provide warnings or instructions should not extend to a person allegedly injured by a product that someone else freely downloaded and printed. There should be some transactional relationship between the defendant company and the person injured. To allow otherwise would subject those who develop CADs to "limitless liability to an indeterminate class of persons conceivably injured by its negligent acts."[255] Likewise, manufacturers of 3D printers should not be subject to liability for products created through their technology, just as manufacturers of any other type of equipment or tool would not be liable for injuries stemming from goods their products are used to make.[256] In traditional terms, a hammer manufacturer is not liable when a house is defectively constructed with one of its tools.

"Negligence law is malleable, however, and courts have sometimes used it to circumvent core product liability principles."

Negligence law is malleable, however, and courts have sometimes used it to circumvent core product liability principles. The potential for expansions of liability law is particularly high where the person or business that is directly responsible for a harm—such as an individual who pirated, modified, and uploaded a dangerous design—is not a viable defendant. That person's identity may be unknown, or he or she may be outside the court's jurisdiction or lack financial resources to compensate an injured plaintiff. And, as products are precisely duplicated through 3D printing technology, in some instances it may be impossible to distinguish a patent holder's products from copies or counterfeits and to determine who actually made the product alleged to have caused a person's injury. In such situations, courts may be tempted to engage in "deep-pocket jurisprudence."[257]

Courts could, for example, consider imposing liability through negligence principles on the company that designed a product that was scanned, copied, and produced by another. While that may seem far-fetched, a few courts have imposed liability on brand-name manufacturers of prescription drugs for plaintiffs who alleged

injury from a generic version of the product.[258] In the 3D printing context, courts may be tempted to hold the original manufacturer of a product liable when someone copies its design and precisely replicates its product, and that product injures someone. Courts may reason that, given widespread availability of 3D printing technology, it was foreseeable to that company that its defective product would be copied and sold by others. It would be unjust, however, to impose liability on a company that did not make the product at issue or benefit from its sale.

Courts may also apply negligence law to impose liability on a company that designed a product but never made or sold it. For example, in a 2011 case before the Mississippi Supreme Court, a woman had sustained injuries in a car accident that she attributed to a defective seatbelt. She sued the maker of the vehicle she was driving, a 1999 Jeep Cherokee, but Chrysler was in bankruptcy at the time. She also named Honeywell International as a defendant. Years earlier, Honeywell had sold a design for a seatbelt buckle to Chrysler, but Honeywell never manufactured or sold the actual product.

Honeywell argued that the Mississippi Product Liability Act (MPLA) provided the sole remedy for product liability actions, and that the MPLA did not provide for a cause of action against a product designer that neither manufactured nor sold the product at issue. The trial court agreed, finding Honeywell was not a "manufacturer" and granting the company's motion for summary judgment. The Mississippi Supreme Court reversed. While the state high court found that the MPLA provides the exclusive remedy for strict liability claims against manufacturers, it ruled that nonmanufacturing and non-selling designers are subject to common law negligence claims.[259] Such decisions should be particularly concerning to those who develop CADs for 3D printing.

Liability concerns are especially high with respect to 3D-printed medical devices and drugs. Some critics note that when products are made by nontraditional manufacturers, such as doctors, pharmacists, and hospitals, there may be no identifiable entity who is responsible as a "manufacturer."[260] Courts have traditionally found that healthcare providers are subject to medical negligence claims when a patient alleges an injury stemming from medical treatment,[261] not product liability claims. As hospitals begin to use onsite 3D printers to create customized medications, implants, and models for patients, these principles may be called into question.[262] Innovation may be stifled if hospitals face tort liability beyond medical malpractice claims.

"In the 3D printing context, courts may be tempted to hold the original manufacturer of a product liable when someone copies its design and precisely replicates its product, and that product injures someone."

Whether litigation is based in product liability or negligence theories, expert testimony will be essential in 3D printing cases. Jurors will not understand from their own experiences whether there was a reasonable, feasible, safer alternative design. Nor will they be able to evaluate the duty of reasonable care in the context of 3D printing and manufacturing without the aid of expert testimony. Courts will need to serve as gatekeepers, ensuring that expert testimony is reliable.

LITTLE LITIGATION TO DATE

While 3D printing technology is likely to be a recurring issue for courts in the coming years, litigation thus far has been sparse.

At least one manufacturer has faced a class action lawsuit stemming from a 3D-printed medical device.[263] In 2015, a patient sued Align Technology, alleging that the company misrepresented the effectiveness of its customized 3D-printed Invisalign aligners, which are thin, clear plastic removable devices used in orthodontic and restorative dentistry. The patient alleged that her dentist took dental impressions that were sent to and approved by the company, but that the aligners did not correct her specific form of teeth misalignment.[264]

In addition to dismissing the plaintiff's fraud-based claims due to the complaint's failure to identify any specific misrepresentation, the court dismissed claims to the extent they were based on a failure to warn. In so doing, the court applied the learned intermediary doctrine, recognizing that a manufacturer is responsible for conveying information about risks associated with medical devices to physicians who prescribe them, not for directly warning patients. Since the patient did not allege that the dentist was misinformed about the risks of the 3D-printed medical device, the court dismissed the claim.[265] While this case involved a 3D-printed product, it presents a straightforward application of consumer law and product liability principles. It did not reach issues unique to the technology.

"Regulators overseeing product safety will have to determine how to apply and enforce laws that were developed with professional product manufacturers in mind to ordinary people, professionals, and businesses that create products through 3D printing."

Regulation of 3D-Printed Products

Regulators overseeing product safety will have to determine how to apply and enforce laws that were developed with professional product manufacturers in mind to ordinary people, professionals, and businesses that create products through 3D printing. Product liability lawyers have observed that "[a]lthough the temptation may be to rush to regulate the 3D printing space, over-regulation may stifle innovation in this new, evolving and promising technology."[266]

The regulatory framework that will encompass 3D printing technology is still largely unknown. The FDA has approved nearly all 3D-printed medical devices as "substantially equivalent" to already-approved medical devices under Section 510(k) of the Federal Food, Drug, and Cosmetic Act.[267] This process requires manufacturers to demonstrate that their proposed 3D-printed product is at least as safe or effective as an existing device. This approach is encouraging in that it suggests that the FDA is not viewing 3D-printed products as novel technology that raises special concerns. In the future, however, the FDA is likely to be asked to review applications for medical devices and prescription drugs made with 3D printing technology that are wholly new and innovative, which will require more rigorous review.

In December 2017, the FDA issued guidance to manufacturers of 3D-printed medical products.[268] The guidance lays out the agency's current thinking on the technical process that medical device manufacturers should use to design and test products made with additive manufacturing, and what type of information the FDA will expect manufacturers to provide when submitting applications for 510(k) or premarket approval.

The FDA characterizes its recommendations as "leapfrog" guidance, which it views as "serving as a mechanism by which the Agency can share initial thoughts regarding technologies that are likely of public importance early in product development."[269] The agency expects its nonbinding recommendations to change as more information becomes available.[270] The FDA has stated that, as its approvals to date have suggested: "It is anticipated that [additive manufacturing (AM)] devices will generally follow the same regulatory requirements and submission expectations as the classification and/or regulation to which a non-AM device of the same type is subject. In rare cases, AM may raise different questions of safety and/or effectiveness."[271]

"In the future, the FDA plans to explore how its regulatory framework will apply to nontraditional manufacturers, such as surgeons in a hospital operating room or technicians in a university laboratory, who create personalized devices for the patients they are treating."

In the future, the FDA plans to explore how its regulatory framework will apply to nontraditional manufacturers, such as surgeons in a hospital operating room or technicians in a university laboratory, who create personalized devices for the patients they are treating.[272]

Other agencies have not yet acted. Consumer Product Safety Commission (CPSC) staff has indicated several safety

concerns with 3D printers, including "the composition of the filament, the high temperature of the printing process, chemical and particulate emissions during printing, and the safety and durability of the final product during consumer use."[273] CPSC staff has recommended that the Commission consider 3D printing among emerging and future technologies deserving of study and risk assessment.[274] Notably, the January 2017 staff report does not mention adopting new regulations, but appropriately focuses on other tools such as developing voluntary standards and collaborating with stakeholders.

As 3D printing technology advances and becomes more commonplace, the CPSC and other agencies may need to consider how existing reporting and recall obligations apply to those who create CADs or produce 3D-printed products, and whether there are areas where regulations specific to 3D printing technology are necessary to encourage innovation while protecting safety.

The Path Forward

As long as 3D printing largely remains the province of traditional manufacturers, liability mechanisms are not likely to change. As 3D printing moves through the supply chain and the technology eventually reaches the end user, however, the law may evolve. When individuals and businesses make their own products and parts rather than buy them from a traditional manufacturer or seller, product liability theories may no longer fit and negligence may become the new default standard. Courts will need to work through these issues to create effective, balanced standards that fairly determine liability and allocate fault. They should resist pressure to abandon core principles of law when the product at issue in a lawsuit was created through 3D printing. Excessive liability would make 3D printers cost prohibitive by eliminating all but the most advanced and expensive printers from the market, and might discourage consumers and businesses from using 3D printing in ways that would provide significant benefits to individuals and society.

Going forward, government agencies should continue to take a measured approach to 3D products. They should apply the time-tested procedures that were developed for approving, monitoring, and addressing safety concerns related to products manufactured through traditional means unless and until there is a demonstrated need for technology-specific regulations.

"Courts will need to work through these issues to create effective, balanced standards that fairly determine liability and allocate fault."

Other Emerging Technologies: Recent Developments

The first edition of "Torts of the Future," issued in March 2017, explored liability and regulatory issues related to five areas of emerging technology, including autonomous vehicles, the commercial use of drones, private space exploration, the sharing economy, and the Internet of Things. Below are highlights of significant developments that have occurred in those areas since that time.

Autonomous Vehicles

Autonomous vehicle (AV) technology is rapidly advancing. Autonomous vehicles are now operating on the roads in Silicon Valley, Phoenix, Pittsburgh, and elsewhere. With more AVs on the road interacting with other drivers and pedestrians, accidents are inevitable, whether as a result of the actions of people or imperfect technology. As discussed below, 2018 began with the first lawsuit stemming from an accident with an AV and, as this report goes to press, the first known fatality stemming from an AV striking a pedestrian occurred and resulted in a quick settlement.[275] Such incidents will test whether the courts, policymakers, manufacturers, and users of AVs respond to concerns without imposing unwarranted liability or regulation that significantly delays a technology that should ultimately make the roads safer by eliminating human error.

FIRST KNOWN LAWSUIT FILED AGAINST AUTONOMOUS VEHICLE MANUFACTURER

In January 2018, the first known lawsuit against a manufacturer was filed over an accident involving an AV.

In that lawsuit, a motorcyclist alleges that he suffered neck and shoulder injuries after a 2016 Chevy Bolt EV knocked him to the ground while traveling on a San Francisco street.[276] General Motors (GM) and its Cruise subsidiary have had a permit to test autonomous vehicles on California roads since June 2015.[277]

According to the complaint, which is just four pages long, a driver was in the front seat but was operating the car in self-

driving mode with his hands off the steering wheel.[278] The operator instructed the Bolt to move from the center to the left lane. The complaint alleges that the motorcyclist, who was traveling directly behind the car in the center lane, attempted to move ahead and pass. As he did, the plaintiff alleges that the Bolt abruptly swerved back into its original lane, striking him and knocking him to the ground.[279]

As is frequently the case in car accidents, there is more than one side to this story. In a report GM filed with California's Department of Motor Vehicles, the automaker explained that the Bolt was driving in the middle lane when it saw a gap and attempted to merge into the left lane.[280] When the minivan ahead of the Bolt in the center lane slowed down, the Bolt abandoned its attempt to merge left. As the Bolt was "re-centering" itself in the middle lane, the plaintiff was approaching the car, "lane-splitting" between the center and right lanes in slow, heavy traffic.[281] As the motorcycle moved into the center lane, it "glanced the side of the Cruise AV, wobbled, and fell over," GM's report said.[282] The San Francisco Police Department police report indicates that the motorcyclist was at fault for attempting to overtake and pass another vehicle on the right before it was safe to do so, but the motorcyclist's attorney also says the police report supports the motorcyclist's version of the events.[283]

The lawsuit names only GM as a defendant; it does not claim the Bolt's operator contributed to the accident. The sole claim, however, is negligence, making the lawsuit more like a traditional auto accident claim than a product liability claim that alleges that a vehicle was defectively designed. The complaint alleges that General Motors owed the plaintiff a duty to "hav[e] its Self-Driving Vehicle operate in a manner in which it obeys the traffic laws and regulations," and breached that duty "in that its Self-Driving Vehicle drove in such a negligent manner that it veered into an adjacent lane of traffic without regard for a passing motorist…."[284] If the case proceeds to trial, the plaintiff may argue that the Bolt failed to perform as a reasonable person would in similar circumstances. Basically, the lawsuit treats the AV much like a person, rather than as a product.

The lawsuit, which seeks unspecified damages as well as attorneys' fees and punitive damages, is pending in the U.S. District Court in San Francisco. It remains to be seen whether the vehicle recorded and stored video or other data that will show precisely what occurred and can be produced in discovery, and whether the parties settle or proceed to trial.

> *"The lawsuit suggests that as cars become autonomous, attorneys whose bread-and-butter work is auto accident claims may continue to bring traditional negligence claims, rather than complex product liability lawsuits…"*

The lawsuit suggests that as cars become autonomous, attorneys whose bread-and-butter work is auto accident claims may continue to bring traditional negligence claims, rather than complex product liability lawsuits that likely necessitate expert testimony on auto design and autonomous technology. One thing appears certain, however: auto manufacturers who incorporate autonomous technology into their vehicles are increasingly likely to be named as defendants in motor vehicle accident cases.

NEW NHTSA REGULATORY GUIDANCE

On September 12, 2017, the National Highway Transportation and Safety Administration (NHTSA) released a new voluntary guidance entitled "Automated Driving Systems: A Vision for Safety 2.0."[285] The new 36-page guidance replaces and significantly pares down the 2016 NHTSA guidance issued by the Obama Administration. It eases the process for manufacturing, testing, and deploying AVs while discouraging states from implementing potentially conflicting AV regulations.

NHTSA's Safety 2.0 focuses on automation levels three to five (Conditional, High, and Full Automation) and covers all vehicles under the agency's jurisdiction. The guidance describes 12 "priority safety elements"[286] for consideration in the design, development, testing, and deployment of AV technologies. The guidance encourages companies engaged in testing and deploying of AVs to submit to NHSTA "Voluntary Safety Self-Assessment" letters demonstrating how they have addressed the safety elements. The guidance, however, makes clear that these letters are not required.

Safety 2.0 distinguishes the roles of the federal and state governments in regulating AVs. NHTSA is solely responsible for regulating the safety, design, and performance aspects of motor vehicles, while states are responsible for regulating the human driver and vehicle operations. NHTSA's guidance provides a "best practices" framework that states may use in drafting applicable laws and regulations. When states craft such laws and regulations, NHTSA encourages them to (1) provide a "technology-neutral" environment, (2) provide licensing and registration procedures for AVs, (3) provide reporting and communication mechanisms to public safety organizations, and (4) review traffic laws that may serve as barriers to the operation of AVs.

NHTSA is already updating its guidance for "Safety 3.0," which will emphasize a unified intermodal approach to automated driving systems policies.[287] The agency sought input on the new guidance at a March 1, 2018, AV summit.[288]

LEGISLATIVE ADVANCES

As NHTSA releases and updates its guidance, Congress has also taken up the issue of AVs. If proposed legislation becomes law, it may help accelerate AV deployment.

In September 2017, the U.S. House of Representatives passed the Safely Ensuring Lives Future Deployment and Research In Vehicle Evolution Act, or the SELF DRIVE Act, with broad bipartisan support.[289] The Senate has its own AV legislation pending, the American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act.[290] The Senate Committee on

> *The preemption provision is considered particularly essential, since introducing AVs will become increasingly complicated as more states enact their own laws.*

Commerce, Science, and Transportation favorably reported the bill in October 2017.

While there are differences in the Senate and House bills, they both provide the federal government with a framework for developing AV rules. They charge NHTSA with regulating the design, construction, and performance of the vehicles, with the goal of encouraging their testing and deployment. The bills would authorize NHTSA to update Federal Motor Vehicle Safety Standards and grant exemptions where needed, and both would require automakers to develop cybersecurity plans. They would preempt state laws in the areas regulated by NHTSA, while preserving the states' traditional authority to regulate registration, licensing, insurance, law enforcement, and traffic laws. The preemption provision is considered particularly essential, since introducing AVs will become increasingly complicated as more states enact their own laws.

STATES MOVING FORWARD

Calls for preemption are warranted, as at least 41 states and the District of Columbia have considered AV legislation over the past seven years.[291] Twenty-one states have passed such laws,[292] and governors in six states have issued executive orders related to AVs.[293] State rules for testing AVs on public roads can vary, from requiring a person in the driver's seat at all times to requiring no human driver in the car.

Fully autonomous vehicles are already operating in states such as Arizona, Florida, Michigan, and Pennsylvania.[294] California is the most recent state to change its rules. As of April 2018, AVs can be tested on public roads in the Golden State without a driver behind the wheel.[295] Under previous rules in place since 2014, AVs could be tested in the state only with a driver sitting behind the wheel who is able to take

> *[A]t least 41 states and the District of Columbia have considered AV legislation over the past seven years. Twenty-one states have passed such laws, and governors in six states have issued executive orders related to AVs.*

control if needed. The California Department of Motor Vehicles issued 50 Autonomous Vehicle Testing Permits to various companies under the 2014 rules.[296]

Commercial Use of Drones

There has been steady progress in broadening the commercial use of drones, but the technology continues to encounter regulatory and litigation turbulence.

MODEL TORT LAW FOR DRONES

As the use of drones continues to grow, incidents leading to litigation are inevitable, but how tort law applies remains unsettled in the courts. To address uncertainty and to provide greater uniformity, the National Conference of Commissioners on Uniform State Laws appointed a committee to draft a model law that would address tort liability and defenses associated with the use of drones.[297] A goal of the committee is to harmonize the law before it evolves in a disjointed manner. The drafting committee is in the early stages of drafting the model act and held its second of four drafting sessions in March 2018. The current outline of the act covers aerial trespass, physical and constructive invasion of privacy, nuisance, intentional torts, strict liability for unmanned aircraft goods and services, and limitations on liability.[298]

As discussed in the 2017 "Torts of the Future" report, one unsettled area of law is where a landowner's rights in the airspace above his or her land begin and end. The draft aerial trespass provision addresses this subject. The provision suggests that states adopt an automatic right of exclusion for landowners up to 100 feet above ground level or 100 feet above surface improvements, whichever is greater.[299] The landowner would not be required to show that the intrusion substantially interfered with enjoyment of the land as required under current aerial trespass law,[300] and since the exclusion is limited to 100 feet, drones would be able to transit above the property at or above that level without exposing the drone's owner to trespass liability.

On the other hand, the draft model act's invasion of privacy provision does not contain an altitude limit. The act would, however, require a showing that the drone's presence violated a person's reasonable expectation of privacy or was offensive to a reasonable person.[301] According to commentary that accompanies the draft, these privacy provisions were modeled after California and Florida laws.

Other model act provisions remain under development, including sections addressing nuisance law, intentional torts, when manufacturers are subject to strict liability

"To address uncertainty and to provide greater uniformity, the National Conference of Commissioners on Uniform State Laws appointed a committee to draft a model law that would address tort liability and defenses associated with the use of drones."

for damages resulting from defective drones, and limitations on the liability of landowners and occupants when trespassing drones fly over their property.

STATES ENACT LAWS REGULATING DRONES

According to the National Conference of State Legislatures, every state legislature has considered legislation related to drones. Currently, 41 states have laws that address drone use and an additional three states adopted resolutions in 2018 to address this issue.[302] These laws touch areas including preemption of local and municipal laws, privacy rights, commercial and governmental uses of drones, criminal penalties for misuse, and uses related to hunting and fishing.

A federal court, however, recently sent a cautionary message to state and local governments as they consider adopting their own regulations on drone use and operations. In September 2017, a federal court invalidated a local ordinance that would have "essentially constitute[d] a wholesale ban on drone use" in the City of Newton, Massachusetts.[303] A lawsuit was filed by a local resident who is a Federal Aviation Administration (FAA) certified small unmanned aircraft pilot. It challenged portions of the ordinance (1) requiring the registration of drones with the City Clerk's office, (2) prohibiting flights below 400 feet over private property without the property owner's express permission, (3) prohibiting flights over public property without the city's permission, and (4) prohibiting any operations beyond the pilot's visual line of sight. The U.S. District Court of Massachusetts held that the local ordinance was preempted, as it "thwarts not only the FAA's objectives, but also those of Congress for the FAA to integrate drones into the national airspace."[304]

> *"Currently, 41 states have laws that address drone use and an additional three states adopted resolutions in 2018 to address this issue."*

FEDERAL REGULATORS SEEK WAYS TO SAFELY LESSEN REGULATORY BURDENS

The White House and Department of Transportation (DOT) are calling for state, local, and tribal governments to submit proposals to test drones within their jurisdictions. In October 2017, they announced an Unmanned Aircraft System Integration Pilot Program.[305] The DOT will enter agreements with these governments to establish innovation zones for testing complex drone operation and to attempt different models for integrating drones into local airspace. The pilot program's stated purpose is to enable the development of drone technologies for use in agriculture, commerce, emergency management, human transportation, and other sectors. According to Transportation Secretary Elaine Chao, the program has received "overwhelming" interest. Selections for the program are expected by May 2018 and the first round of approved pilot programs will likely include at least ten lead participants.[306]

Meanwhile, the FAA has shown increased confidence in drone safety and a willingness to approve waivers that allow drone use in conditions not otherwise permitted by current regulations. For example, for one day in January 2017, the FAA approved the use of commercial drones at the Atlanta Airport.[307] It marked the first time civilian drone flights were given FAA approval in a Class B airspace, which is the designation given to the busiest area around a crowded airport. The drone flights helped map plans for two new parking garages and for relocating a public transit station. According to the project's developer, the drones helped measure and plan the project much faster than standard methods.

Efforts to develop the technology needed to safely expand drone use are ongoing. In December 2017, the FAA's Unmanned Aviation System Identification and Tracking Aviation Rulemaking Committee (ARC) released a final report that detailed its recommendations to the agency.[308] The FAA had chartered the ARC to assist in developing standards for the remote identification and tracking of unmanned aircraft systems (UAS). The ARC included members of the aviation community, industry organizations, law enforcement agencies, public safety organizations, manufacturers, researchers, and entities involved with UAS.

The ARC recommended two methods for UAS to provide remote ID and tracking information to public authorities: (1) direct broadcast (transmitting data in one direction only with no specific destination or recipient) and (2) network publishing (transmitting data to an internet service or group of services).[309] Both methods would send the data to an FAA-approved internet-based database. The ARC recommended a tiered structure to determine whether UAS need to comply with the broadcast or network publication requirement (or both). The ARC could not reach consensus, however, on what threshold of UAS operations would be subject to ID and tracking requirements.

CONGRESS REINSTATES REGISTRATION RULE

The FAA's mandatory regulations for drones in commercial use remain in effect, but its attempt to require owners of model aircraft operated for recreational purposes to register with the agency was briefly in jeopardy. In May 2017, in response to a lawsuit by a D.C. area model aircraft hobbyist, the court found that the FAA's "Registration Rule" directly violated Section 335(a) of the FAA Modernization and Reform Act of 2012, which prohibited the FAA from promulgating any rule or regulation regarding a model aircraft.[310] Congress responded, however, in the National Defense Authorization Act (NDAA), which included language that granted the FAA authority to require registration of civilian small unmanned aircraft, or "model aircraft."[311] Section 1092(d) of the NDAA authorized the FAA to require such registration and reinstated the Registration Rule.

> *Georgia joined a chorus of states that have enacted laws designed to attract companies to locate spaceflight operations by limiting their potential liability.*

Private Space Exploration

In May 2017, Georgia joined a chorus of states that have enacted laws designed to attract companies to locate spaceflight operations by limiting their potential liability. That month, Gov. Nathan Deal signed the Georgia Space Flight Act, declaring the new law will make Spaceport Camden "the best place in the nation to launch a rocket" and will further enhance the state's reputation as a place to do business.[312] The new law ensures that all those who board spacecraft are informed of, and accept, the inherent risks.[313] Space flight operators remain liable to those who fly for injuries caused as a result of the operator's gross negligence for the safety of the participant or intentional misconduct. As discussed in the 2017 "Torts of the Future" report, California, Colorado, Florida, Oklahoma, New Mexico, Texas, and Virginia have enacted similar laws.

At the federal level, legislators and policymakers are focusing on implementing a long-term vision for the National Aeronautics and Space Administration (NASA) that reduces regulatory barriers to private space exploration. The Trump Administration reinstated the National Space Council in June 2017.[314] Led by Vice President Mike Pence, the council held its second meeting in February 2018 at the Kennedy Space Center.[315] The council is concentrating on streamlining regulations in four areas: (1) reforming launch licensing requirements; (2) creating a "one-stop-shop for space commerce" at the Commerce Department and a new undersecretary for space commerce who would oversee specialized activities in space; (3) making it easier for companies to obtain and coordinate radio frequencies that they need to communicate with their satellites; and (4) reducing strict regulations on exporting space-related technologies, many of which are treated as weapons, so that their developers can work more closely with international partners and do business abroad.[316]

In 2017 Congress passed legislation that allows the commercial sector to use NASA's facilities and recognizes the need for NASA to transfer some of its duties to the commercial sector.[317] Soon after, the chairman of the House Science Committee, Rep. Lamar Smith (R-TX), introduced the American Space Commerce Free Enterprise Act with bipartisan support.[318] The bill, which was immediately reported out of committee, advances some of the areas that the National Space Council is considering, such as creating a single authority for nongovernmental space activities housed in the Department of Commerce. It would direct the secretary of commerce to establish a Private Space Activity Advisory Committee to analyze the status and recent developments of nongovernmental space activities, and advise the government on matters relating to U.S. private sector activities in outer space. The bill would reduce the regulatory

barriers that face space companies by reforming the certification and regulatory process for space-based remote sensing technology and by providing greater certainty on compliance with Outer Space Treaty obligations (which can impact the ability to retrieve resources from space), among other areas.[319]

The Sharing Economy

The sharing economy, which allows people to generate income from underused assets, such as cars and spare rooms, continues to grow and expand into new sectors. Smartphones, internet connectivity, and cloud computing all allow consumers to efficiently search for and share goods and services. As this interconnectivity helps bring buyers and suppliers together at much lower costs, it can also create privacy and data security concerns. Platforms in the sharing economy will need to recognize these concerns and take steps to reasonably protect their users' data.

FTC ENFORCEMENT OF PRIVACY AND DATA SECURITY IN THE SHARING ECONOMY

The FTC settled its first enforcement action regarding data security practices in the sharing economy in August, 2017.[320] In its complaint, the FTC alleged that Uber misrepresented the extent to which it monitored its employees' access to personal information about users and drivers and the security measures taken to secure personal information.[321]

Under the terms of the consent order, Uber agreed to implement a comprehensive privacy program and to undergo independent third-party privacy and security audits of its privacy program on a regular basis for the next 20 years.[322] Uber must also keep detailed accounting, personnel, and consumer complaint records for the next 20 years. Under the agreement, Uber will not pay a fine, but it could face monetary penalties if it fails to follow the terms of the agreement.

Of note, the FTC took the position in its complaint that both Uber drivers and its riders were "consumers" of the ride-sharing service. This allows the FTC to extend protection to both parties under Section 5 of the FTC Act, which prohibits unfair or deceptive business conduct, even though Uber views its drivers as independent contractors. While the FTC's position was not tested in court, it could have an impact on other sharing economy services. For example, with home-sharing services, the FTC could take a similar position that the home provider and renter are both consumers, or it could take the approach that only the renter of the home is the consumer and pursue the homeowner and app provider for alleged unfair or deceptive conduct.

The FTC also took an expansive view of personal information, finding it includes personally identifiable information (PII) collected or received, directly or indirectly, as well as geolocation information for an

"The FTC settled its first enforcement action regarding data security practices in the sharing economy."

individual or mobile device. The settlement demonstrates that the FTC intends to hold companies to the privacy promises they make to consumers and require that they protect personal data, even when using a third-party data storage vendor.

RIDE- AND HOME-SHARING GROW WHILE FACING CONTINUED LITIGATION

Ride-sharing (Uber and Lyft) and home-sharing (Airbnb, VRBO, Homeaway) continue to lead the way as the sharing economy grows. Uber is now in over 600 cities in 82 countries, an increase of roughly 100 cities since the 2017 "Torts of the Future" report.[323] In addition, last summer, Gov. Andrew Cuomo signed legislation that allows ride-sharing services outside the New York City area, in places like Long Island and Upstate New York, which were among the last places in the United States in which they were prohibited.[324]

As discussed in the 2017 "Torts of the Future" report, however, these services continue to face significant litigation. Home-sharing services, for example, are confronted by states, counties, cities, and even individual buildings that are seeking to license, regulate, tax, or entirely stop those who offer homes or apartments for short-term rentals from operating.[325] Ride-sharing services continue to face litigation over whether their drivers are independent contractors or employees,[326] claims of unlawful competition,[327] and fair wage disputes.[328]

The Internet of Things

As technology develops, the number of connected devices continues to multiply. Traditionally disconnected products, such as televisions, lights, baby monitors, and toys, are increasingly gaining internet connectivity and becoming "smart" devices, collectively composing the Internet of Things (IoT). With more devices collecting and sharing potentially sensitive data, the FTC is widening its enforcement net to address concern over whether these new devices contain reasonable security measures.

FTC ENFORCEMENT OF THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

On June 21, 2017, the FTC released an updated guidance document for complying with the Children's Online Privacy Protection Act (COPPA).[329] The updated guidance identifies connected toys and other IoT devices that collect personal information, such as voice recordings or geolocation data, as covered under COPPA. The revised guidance also provided two newly approved methods for companies that sell such devices to obtain parental consent to PII collection and sharing: (1) asking knowledge-based authentication questions and (2) using facial recognition to obtain a match with a verified photo ID.[330]

On October 23, 2017, the FTC issued further COPPA guidance regarding the collection of children's audio voice recordings. The guidance clarified that the FTC would not take enforcement action against an IoT device maker when (1) the child's voice was recorded solely to replace written words, such as to perform a search or fulfill a verbal instruction; and (2) the recording was retained for a brief period of time and only for that purpose. To fall

within this exception, the audio that was obtained could not contain personal information, and in its privacy policy the company must still provide clear notice of its collection and use of audio files and its deletion policy.[331]

The FTC began 2018 by announcing its first settlement of alleged COPPA violations arising from internet-connected toys.[332] The FTC had launched its investigation of VTech following a 2015 data breach that affected hundreds of thousands of parents' and children's data from VTech's internet-connected toys.[333] The FTC's complaint alleged that VTech violated COPPA by failing to provide sufficient notice to parents about the information it collected and by failing to establish and follow adequate data security practices. VTech allegedly stated in its privacy policy that the personal information collected would be encrypted, but it did not actually encrypt any of it. As part of the settlement, VTech agreed to pay a $650,000 penalty and for the next 20 years undergo independent, biennial assessments of its comprehensive data security program.[334]

COURT SAYS IF NO INJURY, NO UNFAIRNESS

In January 2017, the FTC brought an action in federal court against D-Link, which makes smart baby monitors. The FTC alleged that the company engaged in unfair and deceptive practices by advertising its routers and cameras as "Easy to Secure" and containing "Advanced Network Security," while flaws in security could allow hackers to easily access consumers' information and cameras. The complaint alleged one count of unfairness relating to D-Link's failure to secure consumers' information and five counts of misrepresentation relating to D-Link's advertising and statements that its routers and internet cameras were secure.[335]

> *"The court's ruling may limit the FTC's ability to bring similar claims against other companies alleging that they placed consumers' information at risk in the absence of an actual breach or allegation that affected consumers suffered a financial loss."*

In September 2017, the U.S. District Court for the Northern District of California dismissed the unfairness claim, finding the FTC failed to allege that the security flaws caused or were likely to cause substantial consumer harm.[336] The court's ruling may limit the FTC's ability to bring similar claims against other companies alleging that they placed consumers' information at risk in the absence of an actual breach or allegation that affected consumers suffered a financial loss.

LITIGATION UPDATE

As discussed in the 2017 "Torts of the Future" report, Toyota and Fiat Chrysler have already been hit with class action lawsuits alleging that their cars' connected systems are susceptible to hacking. Dismissal of one of those suits was affirmed on appeal and the other case appears to be struggling due to the speculative nature of the asserted claims.

In *Cahen v. Toyota Motor Corp.*, the plaintiffs alleged that it was possible to

> *"In 2015, a federal court dismissed the suit for lack of standing, finding that plaintiffs' assertion that their vehicles were worth less as a result of the vulnerability was 'conclusory' and 'speculative.'"*

seize control of a car's throttle, brakes, or steering.[337] In 2015, a federal court dismissed the suit for lack of standing, finding that plaintiffs' assertion that their vehicles were worth less as a result of the vulnerability was "conclusory" and "speculative."[338] The U.S. Court of Appeals for the Ninth Circuit affirmed the dismissal in December 2017, finding that the plaintiffs had made only conclusory allegations that their cars were worth less and had not alleged sufficient facts to establish Article III standing.[339]

Similarly, in 2015 the plaintiffs in *Flynn v. FCA US LLC* filed a lawsuit alleging that some Chrysler models lost value due to vulnerabilities in the connected system that controls the vehicles' phone, navigation, entertainment, and other functions.[340] The lawsuit remains active, but the claims have been significantly pared down. In August 2017, the court dismissed claims that future hacking could cause injury or death, but left intact the plaintiffs' claims that they overpaid for the cars and that the vehicles had depreciated in value in light of the alleged system vulnerabilities.[341]

At a class certification hearing in January 2018, the plaintiffs dropped the loss of value claim, leaving only the overpayment claim.[342] Fiat Chrysler then asked the court to reconsider its motion to dismiss, arguing that absent a loss of resale value, the car owners suffered no injury "[s]ince the plaintiffs received vehicles that are valued the way they expected them to be."[343] Relying on the Ninth Circuit's recent ruling in *Cahen*, the automaker argued that the plaintiffs had not alleged a sufficient-injury-in-fact to establish standing.[344] The court denied reconsideration, but, in April 2018, it took the rare step of certifying an immediate appeal to the Seventh Circuit so that the appellate court might consider whether a future risk of hacking or unauthorized intrusion is too speculative a harm to allow plaintiffs to bring a claim.

LITTLE LEGISLATIVE MOVEMENT

As discussed in the 2017 "Torts of the Future" report, legislators introduced the DIGIT Act and Spy Car Act in Congress in 2016. The Spy Car Act, which would address concerns that cars are collecting data that may not be sufficiently secured, was reintroduced in 2017 by Sen. Ed Markey (D-MA) and Sen. Richard Blumenthal (D-CT), but the bill has failed to advance.[345] The DIGIT Act, which would create a working group of federal agencies to provide recommendations to Congress on how to encourage the growth of IoT, was also reintroduced in 2017. The Senate bill passed the Senate by a voice vote. It was then referred to the House Subcommittee on Communications and Technology, but it has not advanced since August 11, 2017.[346]

In addition, a bipartisan group of U.S. senators introduced the Internet of Things (IoT) Cybersecurity Improvement Act of 2017.[347] The act seeks to impose baseline cybersecurity standards for federal procurement of connected devices. The bill does not, however, apply to consumer devices, and it has not advanced since its introduction in August 2017.

Guiding Principles for Addressing the Liability and Regulatory Implications of Emerging Technologies

The challenge with emerging technologies is to develop a liability and regulatory framework that simultaneously promotes innovation, economic growth, safety, and privacy. Each of the areas profiled in this report—from robotics to 3D printing—promises to bring significant benefits to the public. Excessive liability or heavy-handed regulation, however, can derail or significantly delay new products and services. While each emerging technology faces its own distinct challenges in this regard, certain common themes apply across the board as courts, legislators, and regulators seek to balance innovation and regulation.

Principles of Liability

TRADITIONAL PRINCIPLES OF LIABILITY ADEQUATELY ADDRESS MOST CLAIMS THAT ARISE FROM EMERGING TECHNOLOGIES

The first reported lawsuit stemming from an autonomous vehicle accident, which relies on a traditional negligence claim, supports this thesis. Legislatures should not enact new private rights of action specific to emerging technologies. The Illinois Biometric Information Privacy Act is the only state biometric privacy law to authorize private lawsuits, and has become a poster child for this principle. It has spawned scores of class actions, many of which allege no more than technical violations of the statute.

COURTS SHOULD NOT EXPAND COMMON LAW STANDARDS FOR PRODUCT LIABILITY, PRIVACY VIOLATIONS, OR OTHER CLAIMS IN RESPONSE TO NEW PRODUCTS OR SERVICES

For example, courts should not subject makers of augmented reality applications to trespass, nuisance, or personal injury claims where they are not supported by existing law, or subject them to liability for the careless or criminal acts of others. Nor should courts depart from traditional application of the learned intermediary doctrine when healthcare providers use robotics in surgery, as occurred in Washington State. Individuals and businesses that design or manufacture products should not be subject to liability when their goods are made or copied by others through 3D printing, and the reproductions cause harm.

COURTS SHOULD APPLY CONSTITUTIONAL PRINCIPLES OF STANDING TO PRECLUDE LAWSUITS SEEKING RECOVERY FOR SPECULATIVE FEAR OF FUTURE HARM

As courts have recognized, a theoretical or hypothetical vulnerability in a connected product—whether it is an automobile, children's toy, or fitness device—does not give rise to a viable claim absent actual harm to a consumer.

WHERE LIABILITY EXPOSURE THREATENS AN EMERGING TECHNOLOGY'S VIABILILITY, LEGISLATORS SHOULD ADOPT REASONABLE CONSTRAINTS ON LIABILITY

For example, Georgia is the most recent state to place bounds on liability involving private space travel, recognizing the potential for extraordinary losses and the inherent risks of the activity.

COURTS SHOULD CONSIDER WHETHER STATE LAWS ARE PREEMPTED WHEN AN EMERGING TECHNOLOGY IS REGULATED BY FEDERAL LAW

Overlapping and potentially conflicting federal, state, and local regulation of autonomous vehicles and drone operation, for example, is likely to pose serious impediments to deploying these new technologies. Such a legal patchwork creates an unreasonable risk that a manufacturer or user may inadvertently violate the law and become subject to liability. Federal agencies can prevent this problem by clearly asserting their intent to preempt state law in regulations, agency guidance, and amicus briefs filed with courts.

COURTS SHOULD BE CAUTIOUS OF ATTEMPTS TO REGULATE THROUGH LITIGATION

For instance, courts should reject claims that virtual reality games with violent content lead to violence in real life, and instead adhere to traditional tort principles and legal precedent.

Principles of Regulation

POLICYMAKERS SHOULD NOT REFLEXIVELY RESPOND TO CONCERNS BY BANNING PRODUCTS OR SERVICES OR IMPOSING UNDULY BURDENSOME PERMITTING, REGISTRATION, OR OTHER REGULATORY REQUIREMENTS

For instance, the FDA has taken a balanced approach to mobile medical applications, focusing its oversight on a subset of apps that present the greatest risk to patients if they do not work as intended, while reserving its enforcement discretion to address low-risk mobile health tools and general wellness products. The FDA has also reviewed and approved 3D-printed medical devices in the same manner as

other technologies, and has occasionally granted emergency exemptions from regulations to allow patients to benefit from devices that are not yet approved. On the other hand, a single traffic accident involving an autonomous vehicle, while tragic, should not spur an immediate ban on testing them.

AGENCIES SHOULD AVOID IMPOSING REGULATIONS BASED ON SPECULATIVE RISKS, RATHER THAN ACTUAL PROBLEMS

Congress has adopted a "learning period" that prohibits the FAA from regulating the safety of commercial spaceflights until 2023, as discussed in the 2017 "Torts of the Future" report. This law is intended to avoid imposing regulations based on limited data that would stifle the growing industry, particularly when commercial human spaceflight has yet to begin. The law allows the FAA to step in earlier if there is a serious injury or fatality. It may provide a model for addressing regulation of other emerging technologies. Where already-dense regulations pose an obstacle to the ability of companies to offer innovative products or services, such as in the financial sector, policymakers should consider implementing "regulatory sandboxes," where innovators and regulators work closely together to bring new products to market that benefit consumers.[348]

STATE AND LOCAL GOVERNMENTS SHOULD AVOID IMPOSING REGULATIONS ON AN EMERGING TECHNOLOGY WHEN FEDERAL AGENCIES HAVE ACTED OR ARE ACTIVELY CONSIDERING THE ISSUE

As Congress and the National Highway Traffic Safety Administration develop guidance and regulations governing the safety, design, performance, and testing of autonomous vehicles, states should refrain from regulating such areas. Instead, states should continue their traditional role of regulating licensing and registration, and enforcing traffic laws.

WHEN REGULATION IS WARRANTED, IT SHOULD BE DEVELOPED IN COLLABORATION WITH STAKEHOLDERS WHO FULLY UNDERSTAND THE EMERGING TECHNOLOGY

The reconstituted National Space Council, for example, includes former astronauts, aerospace and commercial spaceflight industry executives, policymakers, and scholars. This type of collaborative process is more likely to result in sound policies, facilitate growth of emerging technologies, and bolster consumer confidence.

BUSINESSES RECOGNIZE THAT IT IS IN THEIR SELF-INTEREST TO TAKE ACTIONS THAT PROMOTE SAFETY AND INSPIRE CONSUMER CONFIDENCE IN THEIR PRODUCTS AND SERVICES

It is in the interest of manufacturers of virtual reality technologies, for example, to provide users with complete instructions for operating VR devices safely, warn them of risks, and enable them to consent to content, in addition to incorporating safety features into the device's design.

Endnotes

1 Hannah Osborne, Stephen Hawking AI Warning: Artificial Intelligence Could Destroy Civilization, Newsweek, Nov. 7, 2017 (quoting remarks of Stephen Hawking at a technology conference in Lisbon, Portugal).

2 *See* Nick Wingham, Elon Musk Says Humanity Needs to Act NOW to Stop Artificial Intelligence and Killer Robots Wiping Us Out, The Sun (U.K.), July 17, 2017.

3 Jasper Hamill, Elon Musk Says Artificial Intelligence and Killer Computers are Far More Dangerous Than North Korea, The Sun (U.K.), Aug. 14, 2017.

4 Tia Ghose, Elon Musk: Regulate AI Before Robots Start 'Killing People', Live Science, July 17, 2017 (quoting Musk comments to National Governors Association).

5 *See* George Harrison, Hackers Could Program Sex Robots to Kill, N.Y. Post, Sept. 11, 2017 (reporting comments of Dr. Nick Patterson, a cybersecurity expert).

6 *See* John Markoff & Claire Cain Miller, As Robotics Advances, Worries of Killer Robots Rise, N.Y. Times, June 16, 2014.

7 Assoc. Press, Jury Awards $10 Million in Killing by Robot, N.Y. Times, Aug. 11, 1983; *see also* Theo Priestley, Is This A Killer Robot Uprising ? Hardly!, Forbes, July 2, 2015 (revisiting Robert Williams' case). Another early case is that of Kenji Urada, a 37-year old factory worker, who entered a restricted zone at a Kawasaki motorcycle plant in 1981 to perform maintenance on a robot without fully turning it off. The robot's powerful hydraulic arm pushed the engineer into an adjacent machine, killing him instantly. *See* Yueh-Hsuan Weng, Chien-Hsun Chen & Chuen-Tsai Sun, Towards the Human-Robot Co-Existence Society: On Safety Intelligence for Next Generation Robots, 1 Int. J. Soc. Robot 267, 273 (2009).

8 Complaint, *Holbrook v. Prodomax Automation Ltd.*, No. 1:17-cv-00219, at 3 (W.D. Mich. filed Mar. 7, 2017).

9 *See* Christopher Brennan, Michigan Woman Killed by Robot with Defect, Suit Says, N.Y. Daily News, Mar. 14, 2017; *see also* Tresa Baldas, A Defective Robot Killed a Woman, a Lawsuit Claims, and Her Family Wants Answers, USA Today, Mar. 15, 2017. Another recent case is that of 22-year-old contractor at a Volkswagen plant in Germany who was killed when a stationary robot he was installing that ordinarily grabs and installs auto parts in a confined area of the factory grabbed him and crushed him against a metal plate, possibly as a result of human error. *See* Abby Philips, Robot Grabs Man, Kills Him in German Car Factory, Wash. Post, July 2, 2015.

10 U.S. Dep't of Labor, Occupational Safety & Health Administration, Fatality and Catastrophe Investigation Summaries, Accident Search Results, Abstract: Robot or Robotics, Mar. 1, 1988 to Mar. 13, 2018 (Mar. 13, 2017); *see also* Markoff & Miller, *supra* (citing OSHA statistics indicating at least 33 workers suffered fatal injuries while working with robot between 1996 and 2011 and providing examples of robot accidents during this period).

11 *See* Occupational Safety & Health Admin., Census of Fatal Occupational Injuries Charts, 1992-2016 (final data). In 2016, three-quarters of workplace fatalities resulted from transportation incidents such as roadway accidents (40%), violent acts by people or animals (17%), and slips, trips, and falls (16%). "Contact with objects and equipment," which includes fatalities associated with robots, accounted for about 15% of fatal occupational injuries. *See id.*

12 *See* Juliann Walsh, Rise of the Cobots, Risk and Insurance, May 2, 2017.

13 *See id.*

14 *See* Harriet Taylor, Lowe's Introduces LoweBot, a New Autonomous In-Store Robot, CNBC, Aug. 30, 2016.

15 Edelman & Edelman, P.C., What Would You Do If a Robot Injured You on the Construction Site?, EdlemanPCLaw.com (blog), May 24, 2017.

16 *See* Olivier Oullier, The Force is Real: How 'Star Wars' Neuroscience is Revolutionizing Healthcare and More, Fortune, Jan. 4, 2018.

17 *See, e.g.*, Swartz & Swartz, P.C., Robotic Surgery Malpractice, at https://www.swartzlaw.com/robotic-surgery-malpractice.html (last visited Mar. 1, 2018); Spencer Morgan Law, When Robot Doctors Injure, Who is to Blame: The Hospital or the Patient, at https://smorganlaw.com/when-robot-doctors-injure-who-is-to-blame-the-hospital-or-the-patient/ (last visited Mar. 1, 2018).

18 *See* Intuitive Surgical, Inc., Form 10-K for the Quarterly Period Ended December 31, 2017, at 82 (filed Feb. 2, 2018).

19 For example, the manufacturer settled one such case during deliberations after plaintiffs' lawyers urged a California jury to award their client $30 million in 2016. *See* Brandon Lowery, Intuitive Cuts Deal Before Jury Verdict in $30M Robot Trial, Law360, Apr. 20, 2016 (discussing *Zarick v. Intuitive Surgery Inc.*, No. 1-12-cv-237723 (Cal. Super. Ct., County of Santa Clara).

20 *See Taylor v. Intuitive Surgical, Inc.*, 389 P.3d 517 (Wash. 2017).

21 Julie A. Steinberg, Will More States Require Device Makers to Warn Hospitals?, 45 Prod. Safety Liab. Rep. 174 (Bloomberg BNA), Feb. 20, 2017 (quoting Richard Friedman, the lead plaintiffs' counsel in *Taylor*).

22 *See* Intuitive Surgical, Inc., Form 10-K for the Quarterly Period Ended December 31, 2017, at 83 (filed Feb. 2, 2018).

23 *See, e.g.*, Erin Bosman, Julie Park & Austin Marsh, What the Intuitive Ruling Means for Medical Device Makers, Law360, Mar. 1, 2017.

24 Julie A. Steinberg, Will More States Require Device Makers to Warn Hospitals?, 45 Prod. Safety Liab. Rep. 174 (Bloomberg BNA), Feb. 20, 2017 (quoting Richard Friedman, the lead plaintiffs' counsel in *Taylor*).

25 *See id.*

26 *See* Meera Senthilingam, Are Autonomous Robots Your Next Surgeons?, CNN, May 12, 2016; Andrew M. Seaman, Completely Automated Robotic Surgery: On the Horizon?, Reuters, May 10, 2016.

27 *See* James Beck, If the Surgeon's a Robot, Who's the Learned Intermediary?, Law360, July 31, 2017.

28 *See* Whitney Richardson & Brian X. Chen, CES 2018: What the Gadget Fest Looks Like in 'the Year of A.I.', N.Y. Times, Jan. 11, 2018.

29 *See* Andrew Gebhart, The Robots of CES 2018: Cuteness Reigns Supreme, CNet, Jan. 12, 2018; Andrew Gebhart, Aeolus is the Smart Home Robot of My Dreams, Jan. 8, 2018.

30 *Register.com, Inc. v. Verio, Inc.*, 356 F.3d 393 (2d Cir. 2004). The court also ruled that the domain registrar that sued was likely to prevail on its claim that repeated use of the search robots to gather data from its database constituted a trespass to chattels.

31 *See* Joel Espelien, The Brave New World of Robot Law, ABA Law Practice Today, Jan. 14, 2016 (suggesting this possibility).

32 *See generally* Enrique Schaerer, Richard Kelley & Monica Nicolescu, Robots as Animals: A Framework for Liability and Responsibility in Human-Robot Interactions, 18th IEEE International Symposium on Robot and Human Interactive Communication (2009).

33 *See* Victor E. Schwartz et al., Prosser, Wade & Schwartz's Torts 1-2 (13th ed. 2015).

34 *See, e.g.*, John Frank Weaver, Robots Are People, Too, Slate, July 27, 2014.

35 *See* Annalle Newitz, Robots Need Civil Rights, Too, Boston Globe, Sept. 8, 2017; *see also* Ryan Calo, When a Robot Kills, Is It Murder or Product Liability?, Slate, Apr. 26, 2016 (responding to Paolo Bacigalupi's short story, Mika Model, in which a leased "sexbot" that claims to experience pain and emotions requests a lawyer after killing an abusive man).

36 *See Central Hudson Gas & Electric Corp. v. Public Serv. Comm'n*, 447 U.S. 557 (1980) (invalidating state regulation banning promotional advertising by utility).

37 *See Burwell v. Hobby Lobby*, 134 S. Ct. 2751 (2014) (holding that, as applied to closely held corporations, federal regulations requiring employers to provide female employees with no-cost access to contraception violate the Religious Freedom Restoration Act).

38 *See Citizens United v. Federal Election Comm'n*, 558 U.S. 310 (2010) (recognizing that political spending is a form of protected speech, and government may not keep corporations or unions from spending money to support or denounce individual candidates in elections); *First Nat'l Bank of Boston v. Bellotti* (1978) (defining free speech rights of corporations for the first time, and holding that corporations have a First Amendment right to make contributions to ballot initiative campaigns).

39 *See* Cleve R. Wootson Jr., Saudi Arabia, Which Denies Women Equal Rights, Makes a Robot a Citizen, Wash. Post, Oct. 29, 2017; *see also* Zara Stone, Everything You Need to Know About Sophia, The World's First Robot Citizen, Forbes, Nov. 7, 2017.

40 *See* European Parliament Resolution of 16 February 2017 With Recommendations to the Commission on Civil Law Rules on Robots (2015/2103(INL)).

41 Asimov's Laws are (1) a robot may not injure a human being or, through inaction, allow a human being to come to harm; (2) a robot must obey the orders given to it by human beings except where such orders would conflict with the First Law; and (3) a robot must protect its own existence as long as such protection does not conflict with the First or Second Laws. I. Asimov, Runaround (1942). Asimov later added an addition law, of highest priority, providing that "a robot may not harm humanity, or, by inaction, allow humanity to come to harm." I. Asimov, Robots and Empire (1985).

42 European Parliament Resolution, *supra*, at ¶ X.

43 *Id.* ¶ 52.

44 *Id.* ¶ 56.

45 *Id.*

46 *See id.* ¶ 53.

47 *See id.* ¶ 2.

48 *See id.* ¶59.

49 *See id.* ¶¶ 31-35.

50 *Id.* ¶ 59(f).

51 *See* Giving Robots 'Personhood' is Actually About Making Corporations Accountable, The Verge, Jan. 19, 2017.

52 *See* Charlotte Walker-Osborn & Paula Barrett, Artificial Intelligence: The EU, Liability and the Retail Sector, Robotics L.J., May 8, 2017.

53 *See, e.g.*, Jane Wakefield, MEPs Vote on Robots' Legal Status – and If a Kill Switch is Required, BBC, Jan. 12, 2017 (quoting comments of Lorna Brazell, a partner at the law firm Osborne Clarke).

54 *Naruto v. Slater*, No. 15-cv-04324, 2016 WL 362231 (N.D. Cal. Jan. 28, 2016). Ultimately, People for the Ethical Treatment of Animals (PETA), which brought the lawsuit in the name of the monkey, agreed to withdraw an appeal to the Ninth Circuit and David Slater, the photographer, agreed to donate 25 percent of proceeds from sales or usage of the "monkey selfies" to charities in Indonesia that protect crested macaques. *See* Amy B. Wang, 'Monkey Selfie' Lawsuit Finally Settled After Two Years and a Banana Boat Full of Puns, Wash. Post, Sept. 12, 2017.

55 *See* Chris Kirk, Wii Revolution: How Nintendo Saved Itself from Irrelevance and Turned Everyone into a Gamer, Slate, Oct. 22, 2012.

56 Kif Leswing, 'Pokémon Go' was the Most Downloaded iPhone App Worldwide in 2016, Apple Says, Bus. Insider, Jan. 5, 2017.

57 *See* Bryant Urstadt & Sarah Frier, Welcome to Zuckerworld: Facebook's Really Big Plans for Virtual Reality, Bloomberg Businessweek, July 27, 2016.

58 *See* Lisa Eadicicco, Sony Is Launching a New PlayStation VR Headset, Time, Oct. 2, 2017.

59 *See* CES 2016: HTC Vive Virtual Reality Headset Gets Upgraded, BBC News, Jan. 5, 2016.

60 *See* Jimmy Thang, VR Headsets Specs Compared: HTC Vive, Oculus Rift, PSVR, and More, Gamestop, Feb. 13, 2018.

61 *See id.*

62 *See* Zachary Sherman, The Power and Future of Virtual Reality in the Workplace, Fordham J. of Corp. & Financial Law (blog), Nov. 12, 2017.

63 *See* Nick Boykin, Virginia Beach Realtor Uses Virtual Reality to Show Off Houses, WKTR News 3, Feb 5, 2018.

64 *See* Sarah DiGiulio, 3 Ways Virtual Reality is Transforming Medical Care, NBC Mach, Aug. 22, 2017; John Gaudiosi, This VR Company Helps Soldiers Cope With War Injuries, Fortune, Feb. 22, 2016.

65 *See* Abrar Al-Heeti, This VR Headset Takes a Hard Look at Brain Injuries, CNET, Oct. 25, 2017.

66 Daniel Terdiman, Why 2018 Will Be the Year of VR 2.0, Fast Company, Jan 1, 2018;

67 *See, e.g.*, Scott Stein, 2018 Could be the Year VR Cuts the Cord, CNET, Jan. 24, 2018;

68 *See* Anshel Sag, CES 2018: Virtual Reality And Augmented Reality Get Another Shot, Forbes, Jan. 25, 2018.

69 *See, e.g.*, Schulyer Moore, The Legal Reality of Virtual Reality, Forbes, Mar. 10, 2017.

70 *See* Russian Man Dies from Fall While Wearing Virtual Reality Glasses, Moscow Times, Dec. 22, 2017; *see also* Callum Paton, Virtual Reality Gamer Slips and Dies from Blood Loss After Falling on Glass Table, Newsweek, Dec. 23, 2017.

71 *See* Scott Stein, The Dangers of Virtual Reality, CNET, Mar. 29, 2016.

72 *Id.*

73 *See* C.P. Panayiotopoulos, Video Game-Induced Seizures (VGS) (Epilepsy Foundation, Jan. 1, 2006).

74 *See, e.g.*, Assoc. Press, Jury Doesn't Buy Epileptic Lawsuit Against Nintendo; Prescott Courier, Sept. 19, 1993, at 7A (reporting jury's rejection of lawsuit brought by 20-year-old in Michigan, which Nintendo said was the first case in which it heard of a game triggering a seizure when filed in 1991); Suit Says Nintendo Gave Boy Seizures, Chic. Trib., Jan. 26, 1993 (reporting on filing of a class action lawsuit in Cook County, Illinois, seeking injunction to stop sale of video games on basis they cause seizures).

75 *See* Jessica Solodar, Lawsuits Filed After Games Caused Seizures, Seizures from Video Games (blog), Apr. 6, 2013 (compiling outcomes of cases ten filed between 1991 and 2011).

76 *See* Roya Bagheri, Virtual Reality: The Real Life Consequences, 17 U.C. Davis Bus. L.J. 101,114 (2017).

77 *See* Oculus, Legal Documents, Health and Safety Warnings (last visited Mar. 1, 2018).

78 *See, e.g.*, *Elvig v. Nintendo Am., Inc.*, No. 08-cv-02616, 2010 WL 3803814, at *6-7 (D. Colo. Sept. 23, 2010).

79 Restatement of Torts, Third: Products Liability § 2, cmt. l (1998).

80 *See* Mark A. Lemley & Eugene Volokh, Law, Virtual Reality, and Augmented Reality, 166 Pa. L. Rev. (forthcoming 2018).

81 *See* Sophie Borland, Don't Pokémon Go and Drive! More than 110,000 Road Accidents in the US were Caused by the Game in Just 10 Days, Daily Mail, Sept. 16, 2016 (estimating accidents based on Twitter messages and news reports).

82 *See Rosenberg v. Harwood*, No. 100916536, 2011 WL 3153314, at *1 (D. Utah May 27, 2011).

83 *Id.*

84 *Id.*

85 *See* Fredrick Kunkle, Case Dismissed Against Person Who Texted Driver in Fatal Pennsylvania Crash, Wash. Post, Feb. 3, 2018.

86 *See Kubert v. Best*, 75 A.3d 1214, 1228 (N.J. Super. Ct. App. Div. 2013) (finding a person has a duty not to text a person he or she knows is driving or when the sender has "special reason to know, the recipient will view the text while driving, but finding insufficient evidence to support such knowledge in that case); *see also* Emily K. Strider, Note, Don't Text a Driver: Civil Liability of Remote Third-Party Texters After Kubert v. Best, 56 Will. & Mary L. Rev. 1003 (2015) (examining existing tort law principles and arguing against imposing liability on remote third-party texters as "doing so would extend third-party liability well beyond any articulated and established duty, and would depart from our current understanding of third-party liability").

87 A National Highway Traffic Safety Administration (NHTSA) study has found that eating while driving increases the chance of an accident more than talking on a phone. *See* Maria Vega et al., Understanding the Effects of Distracted Driving and Developing Strategies to Reduce Resulting Deaths and Injuries: A Report to Congress, No. DOT HS 812 053 (Nat'l Highway Traffic Safety Admin., Dec. 2013); *see also* Auto Alliance & Am. Academy of Orthopedic Surgeons, Eating While Driving, DecidetoDrive.org (last visited Mar. 1, 2018) (indicating research shows that a driver who is drinking or eating is 3.6 times more likely to be in an automobile crash than attentive drivers).

88 An exceptional case is the well-known lawsuit against McDonald's in which a woman who was burned by hot coffee that spilled in her lap while driving received a $2.9 million dollar verdict, including $2.7 million in punitive damages. That case focused on whether the coffee was a defective product as a result of its temperature and was not an ordinary distracted driving case, however, the jury did find McDonald's 80 percent at fault and attributed only 20 percent of the responsibility to the plaintiff's negligence. While on appeal, the case settled for a lesser sum. For more information, *see* www.hotcoffeetruth.com.

89 *See, e.g.*, Emily Roseman, Man Gets Ticket for Eating Burger While Driving, WLTX News, Jan. 19, 2015 (reporting that an Alabama man was ticketed after an officer observed him eating a burger from a McDonald's drive thru while driving over the course of two miles).

90 *See, e.g.*, Robinson Salyers PLLC, Accidents Caused by Eating While Behind the Wheel (blog post), Apr. 24, 2017 (indicating that personal injury attorneys search police and other first responder reports for such observations).

91 *See* Ralph L. Jacobson, Are Pokémon Go's Creators Potentially Liable for Injuries Caused by Inattentive Game Players, CJEL Accident Attorneys, July 11, 2016.

92 *See Weirum v. RKO General, Inc.*, 539 P.2d 36, 48 (Cal. 1975).

93 *See id.* at 47-48.

94 *See* Bill Lindelof, 'Pokémon Go' Players Robbed at GunPoint in Elk Grove Park, Sacramento Bee, July 22, 2016; Dan Morse & T. Rees Shapiro, Robbers Target Pokémon Go Players in Maryland and Beyond, Wash. Post, July 13, 2016.

95 Joel Currier, Alleged 'Pokémon Go' Robbers are Charged in St. Louis Crime Spree, St. Louis Post-Dispatch, Apr. 28, 2017; Denise Hollinshed & Christine Byers, Robbers Target Players of Popular 'Pokémon Go' Smartphone Game, Police in O'Fallon, Mo., Say, St. Louis Post-Dispatch, July 11, 2016.

96 *See* Restatement (Second) of Torts § 302B, cmt. d (1965) ("In the ordinary case [a person] may reasonably proceed upon the assumption that others will not interfere in a manner intended to cause harm to anyone. This is true particularly where the intentional conduct is a crime, since under ordinary circumstances it may reasonably be assumed that no one will violate the criminal law.").

97 *See Double Quick, Inc. v. Lymas*, 50 So.3d 292, 298 (Miss. 2010) (reversing $4 million verdict to man who was shot while leaving a convenience store).

98 *See Lymas,* 50 So.3d at 298; *see also* Restatement (Second) of Torts § 302B (1965) ("An act or an omission may be negligent if the actor realizes or should realize that it involves an unreasonable risk of harm to another through the conduct of the other or a third person which is intended to cause harm, even though such conduct is criminal.").

99 The Restatement recognizes that situations in which a person is required to anticipate and guard against intentional, or even criminal, misconduct of others generally arise "where the actor is under a special responsibility toward the one who suffers the harm, which includes the duty to protect him against such intentional misconduct; or where the actor's own affirmative act has created or exposed the other to a recognizable high degree of risk of harm through such misconduct, which a reasonable man would take into account." *See id.* cmt. e.

100 *See Lymas,* 50 So. 3d. at 299.

101 *See James v. Meow Media, Inc.*, 300 F.3d 683, 694 (6th Cir. 2002).

102 Steph Solis, Pokémon Players Shot at in Palm Coast, Fla, USA Today, July 16, 2016.

103 Assoc. Press, Woman: Daughter Hit by Car While Playing 'Pokémon Go', Wash. Times, July 13, 2016.

104 Kimiya Manoochehri, Two Fall from Cliff Reportedly Playing Pokémon Go, USA Today, July 14, 2016.

105 Complaint, *The Villas of Positano Condominium Ass'n Inc. v. Niantic Inc.*, No. 3:16-cv-05091 (N.D. Cal. Sept. 1, 2016); Class Action Complaint, *Dodich v. Niantic*, Inc., No. 3:16-cv-04556 (N.D. Cal. Aug. 10, 2016); Class Action Complaint, *Marder v. Niantic, Inc.*, No. 3:16-cv-04300 (N.D. Cal. July 29, 2016).

106 Marder Complaint, *supra*, at 3.

107 Dodich Complaint, *supra*, at 4.

108 Villas of Positano Complaint, *supra*, at 9-10.

109 Consolidated Amended Class Action Complaint, *In re: Pokémon Go Nuisance Litig.*, No. 3:16-cv-04300, at 3-4 (N.D. Cal. Nov. 25, 2016).

110 *See id.* at 28.

111 Consolidation and Case Management Order, *In re: Pokémon Go Nuisance Litig.*, No. 3:16-cv-04300 (N.D. Cal. Sept. 23, 2016).

112 *See* Allison Grande, 'Pokémon Go' Maker Encouraged Trespassing, Court Told, Law360, Mar. 3, 2017.

113 Transcript of Proceedings, *In re: Pokémon Go Nuisance Litig.*, No. 3:16-cv-04300, at 3-5 (N.D. Cal. July 27, 2017).

114 *See id.* at 8-9.

115 *Id.* at 9.

116 Plaintiffs' Second Consolidated Amended Class Action Complaint, *In re: Pokémon Go Nuisance Litig.*, No. 16-cv-04300 (N.D. Cal. Aug. 28, 2017).

117 Carla Bayles, Pokémon Go Trespass Row Raises Novel Issues, Judge Says, Law360, Mar. 29, 2018 (quoting Judge Donato statement at a March 29, 2018 hearing).

118 Restatement (Second) of Torts § 158 (1965) ("One is subject to liability to another for trespass, irrespective of whether he thereby causes harm to any legally protected interest of the other, if he intentionally . . . enters land in the possession of the other, or *causes a thing or a third person to do so* . . . .") (emphasis added).

119 *See id.* cmt. j ("If, by any act of his, the actor intentionally causes a third person to enter land, he is as fully liable as though he himself enters. Thus, if the actor has commanded or requested a third party enter land in the possession of another, the actor is responsible for the third party's entry if it be a trespass.").

120 *See* Molly Shaffer Van Houweling, Tempting Trespass or Suggesting Sociability? Augmented Reality and the Right to Include, 51 U.C. Davis L. Rev. 731, 737-38 (2017).

121 *See Dietz v. Illinois Bell Tel. Co.*, 507 N.E.2d 24, 25-28 (Ill. App. Ct. 1987) (finding telephone company that instructed cable company to enter plaintiff's land to access poles was not liable for indirect trespass because there were no facts alleged that would establish that the telephone company intended or knew that the cable company would fail to ask for permission to enter, which the cable company was required to do under the license agreement).

122 Van Houweling, 51 U.C. Davis L. Rev. at 740.

123 Restatement (Second) of Torts § 821D.

124 *See* Restatement (Second) of Torts § 822.

125 *See id.* §§ 826; *see also* § 827 (providing factors for evaluating gravity of harm including extent of harm, character of harm, social value that the law attaches to the use or enjoyment of the property, suitability of the particular use or enjoyment invaded to the character of the locality, and the burden on the person harmed of avoiding the harm); § 828 (providing factors for evaluating the utility of the conduct, including its social value, suitability to the character of the locality, and the impracticability of preventing or avoiding the invasion).

126 *Exxon Mobil Corp. v. Albright*, 71 A.3d 30, 94, on reconsideration in part, 71 A.3d 150 (Md. 2013) (internal quotations and alterations omitted).

127 *See, e.g., Schuman v. Greenbelt Homes, Inc.*, 69 A.3d 512, 522 (Md. Ct. Spec. App. 2013) (holding that defendant's smoking on patio

did not pose significant to neighbor where he alleged he could not sit on his porch for up to an hour and a half each evening and has to shut his windows at that time).

128 *See Five Oaks Corp. v. Gathmann*, 58 A.2d 656, 659-61 (Md. 1948).

129 *See, e.g., James v. Meow Media, Inc.*, 300 F.3d 683 (6th Cir. 2002); *Sanders v. Acclaim Entm't, Inc.*, 188 F. Supp. 2d 1264 (D. Colo. 2002); *Wilson v. Midway Games, Inc.*, 198 F. Supp. 2d 167 (D. Conn. 2002).

130 *See Meow Media*, 300 F.3d at 700-01 (holding companies that produced or maintained video games, movies, and Internet websites were not liable for deaths resulting from school shooting perpetrated by classmate).

131 For an interesting article exploring these types of situations, *see* Mark A. Lemley & Eugene Volokh, Law, Virtual Reality, and Augmented Reality, 166 Pa. L. Rev. (forthcoming 2018).

132 *See generally* Jaclyn Seelagy, Virtual Violence, 64 UCLA L. Rev. Discourse 412, 421, 432 (2016) (finding that when a person maliciously uses VR, causing real and physical harm, "the virtual reality used to commit the violent act is merely a new type of weapon" and concluding that "what activity is acceptable, including violence, should be left primarily to users and developers, in the form of consent, user customization, software and hardware limitations, and any other future developments we cannot yet set").

133 *See generally* Declan T. Conroy, Property Rights in Augmented Reality, 24 Mich. Telecomm. & Tech. L. Rev. 17 (2017) (arguing that existing principles of property law should protect real property owners' interest in digital space linked to their property); Samuel Mallick, Note, Augmenting Property Law: Applying the Right to Exclude in the Augmented Reality Universe, 19 Vand. J. Ent. & Tech. L. 1057 (2017) (finding existing remedies are insufficient or would chill development of AR, and arguing that courts should develop property law based on an "open range" model of the right to exclude for virtual intrusions on private land, which would allow the owner to exclude AR by submitted an opt-out request).

134 *See* Lemley & Volokh, supra ("[I]f you're screaming in a VR forum [creating a nuisance] from your apartment in Poland, is it fair to require you to answer lawsuits filed in San Francisco or Buenos Aires?").

135 *See* Maria Korolov, The Real Risks of Virtual Reality, Risk Management, Oct. 1, 2014.

136 *See* Jason Evangelho, Senator Al Franken Wants Answers from Oculus About Its Privacy Policy, Forbes, Apr. 7, 2016.

137 *See* Letter from Senator Al Franken to John Hanke, CEO, Niantic, Inc., July 12, 2016; *see also* Chris Isidore, Al Franken is Worried About Pokemon Go Players' Privacy, CNN, July 13, 2016.

138 *See* Paul Merrion, Franken Sees Reality of Privacy Concerns at Oculus, CQ Roll Call, May 20, 2016.

139 Ben Gilbert, The Team Behind Pokémon Go Assures US Senator that the Game Isn't Violating Your Privacy, Bus. Insider, Sept. 1, 2016 (quoting Niantic's letter in response to Senator Franken).

140 *See* Press Release, Reps. DelBene, Clarke, Flores, Issa and Lieu form Reality Caucus, May 3, 2017; *see also* Selena Larson, Congressional Reps Create a 'Reality Caucus', CNN, May 3, 2017.

141 *See* Consumer Tech. Acc'n, Press Release, 2018 Tech Industry Revenue to Reach Record $351 Billion, Says CTA, Jan. 7, 2018.

142 *See* Leo Sun, Wearables Stocks: What to Watch in 2018, NASDAQ, Jan. 4, 2018.

143 *See* Research 2 Guidance, mHealth App Economics 2017 Current Status and Future Trends in Mobile Health, Nov. 2017.

144 *See id.*

145 *See* FitBit, Why FitBit, at https://www.fitbit.com/whyfitbit.

146 *See id.*

147 *See* Jonha Revesencio, Exploring the Benefits of Wearable Technology, HuffPost, Dec. 6, 2017.

148 *See* Ruth G. Zavitsanos, Motivational Competition, Gratifying Recognition, and Healthy Benefits #Fitbit, HuffPost, Apr. 13, 2017.

149 *See* Becca Caddy, Can a Smartwatch Save Your Life?, TechRadar, Jan. 2018.

150 *See id.*; *see also* Amy O'Leary, An App That Saved 10,000 Lives, N.Y. Times, Oct. 5, 2013.

151 *See* Brian Dolan, Prediction: Health Wearables to Save 1.3 Million Lives by 2020, MobiHealthNews, Dec. 16, 2014.

152 *See* Adam Satariano, Wear This Device so the Boss Knows You're Losing Weight, Bloomberg, Aug. 21, 2014.

153 *See id.; see also* BP Wellness Program, BP Million Step Challenge (250-1,000 points).

154 *See* Parmy Olson, The Quantified Other: Nest And Fitbit Chase A Lucrative Side Business, Forbes, Apr. 17, 2014.

155 *See* Tara Siegel Bernard, Giving Out Private Data for Discount in Insurance, N.Y. Times, Apr. 8, 2015.

156 *See* Lucas Mearian, Insurance Company Now Offers Discounts – If You Let It Track Your Fitbit, Computerworld, Apr. 17, 2015.

157 *See* U.S. Food & Drug Admin., Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff (Feb. 9, 2015).

158 Medical apps that are subject to regulatory oversite include: medical apps that are intended to be used as an accessory or extension of a regulated medical device; medical apps that transform a mobile platform into a regulated medical device by using attachments, display screens, or sensors or by including functionalities similar to those of currently regulated medical devices; and medical apps that become a regulated medical device by performing patient-specific analysis and providing patient-specific diagnosis, or treatment recommendations. *See id.*

159 A medical app meets the definition of a medical device if it is intended to be used to diagnose, cure, mitigate, treat, or prevent disease, or affect the body's structure or function. *See id.*

160 *See* U.S. Food & Drug Admin., General Wellness: Policy for Low Risk Devices Guidance for Industry and Food and Drug Administration Staff (July 29, 2016).

161 *See* FTC, Mobile Health App Developers: FTC Best Practices, Apr. 2016.

162 *See* FTC, Staff Report, Internet of Things: Privacy & Security in a Connected World, Jan. 2015.

163 *See* FTC, Mobile Health Apps Interactive Tool.

164 *See id.*

165 *See* FTC, Transcript, FTC Spring Privacy Series: Consumer Generated and Controlled Health Data, May 7, 2014.

166 *See FTC v. Frostwire, LLC*, 1:11cv-23643-DLD (S.D. Fla. Oct. 12, 2011) (The default setting made users' personal files public); *United States v. Path, Inc.*, No. 3:13-cv-00448-RS (N.D. Cal. Fed. 8, 2013) (The app collected personal info from mobile address books and collected children's info without parental consent).

167 *See* FTC, Press Release, FTC Approves Final Order Settling Charges Against Flashlight App Creator, April 9, 2014.

168 *See, e.g., In the Matter of HTC America, Inc.*, Docket C-4406 (FTC June 25, 2013).

169 *See* FTC, Press Release, "Acne Cure" Mobile App Marketers Will Drop Baseless Claims Under FTC Settlements, Sept. 8, 2011.

170 *See* FTC, Press Release, "Melanoma Detection" App Sellers Barred from Making Deceptive Health Claims, August 13, 2015; FTC, Press Release, FTC Cracks Down on Marketers of "Melanoma Detection" Apps, Feb. 23, 2015.

171 *See id.; see also* FTC, Press Release, Makers of Jungle Rangers Computer Game for Kids Settle FTC Charges that They Deceived Consumers with Baseless "Brain Training" Claims, Jan. 20, 2015 (indicating the makers of Jungle Rangers Computer Game for Kids settled charges that they deceived consumers with baseless claims that the app improves children's focus, memory, attention, behavior, and school performance).

172 *See* Office of California AG, Press Release, Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications, Feb. 22, 2012.

173 740 Ill. Comp. Stat. §§ 14/1 to 14/99.

174 Tex. Bus & Com. Code Ann. § 503.001.

175 Wash. Rev. Code Ann. §§ 19.375.010 to 19.375.900.

176 740 Ill. Comp. Stat. § 14/5(g).

177 740 Ill. Comp. Stat. § 14/10.

178 *See id.*

179 740 Ill. Comp. Stat. § 14/10.

180 *See id.*

181 *See In re Facebook Biometric Info. Privacy Litig.,* 185 F. Supp. 3d 1155 (N.D. Cal. May 5, 2016); *Norberg v. Shutterfly, Inc.,* 152 F. Supp. 3d 1103 (N.D. Ill. Dec. 19, 2015).

182 *See Facebook,* 185 F. Supp. 3d at 1171.

183 *See id.*

184 740 Ill. Comp. Stat. § 14/15.

185 *See id.*

186 740 Ill. Comp. Stat. § 14/20.

187 *See* Tex. Bus & Com. Code Ann. § 503.001(d); Wash. Rev. Code Ann. § 19.375.030.

188 *See McCollough v. Smarte Carte, Inc.*, 2016 WL 4077108 (N.D. Ill. Aug. 1, 2016).

189 *See Rosenbach v. Six Flags Entertainment Corp.*, 2017 WL 6523910 (Ill. App. Ct. Dec. 21, 2017); *see also Vigil v. Take-Two Interactive Software, Inc.*, 235 F.Supp.3d 499 (2017) (court held that procedural violations of the notice and consent provisions of BIPA are not by themselves sufficient to confer standing) *aff'd in part and rev'd in part, Santana v. Take-Two Interactive Software, Inc.*, 2017 WL 5592589 (2d Cir. Nov. 21, 2017) (court affirmed that the plaintiffs lacked standing but reversed the dismissal with prejudice to be without prejudice as the court lacked subject matter jurisdiction).

190 By contrast, Washington's regulation of biometric identifiers is limited in substantive scope to the collection, retention, use, and disclosure of biometric identifiers for a "commercial purpose" only. The statute defines commercial purpose as "a purpose in furtherance of the sale or disclosure to a third party of a biometric identifier for the purpose of marketing of goods and services when such goods or services are unrelated to the initial transaction in which a person first gains possession of an individual's biometric identifier." The statute expressly excludes a "security purpose" such as preventing shoplifting, fraud or any other misappropriation or theft of a thing of value from the definition of a commercial purpose. *See* Wash. Rev. Code Ann. § 19.375.010. The Texas statute is also limited to a commercial purpose, but it does not expressly exclude for a security purpose. *See* Tex. Bus & Com. Code Ann. § 503.001(b).

191 *See* Steven Grimes & Eric Shinabarger, Biometric Privacy Litigation: The Next Class Action Battleground, Bloomberg Law, Jan. 17, 2018.

192 *See* Amy Korte, Airlines Hit with Class-Action Lawsuits under Biometric Privacy Law, Ill. Policy, Nov. 20, 2017.

193 *See* Melissa Daniels, Tanning Co. Settles for $1.5M Under Illinois Biometric Law, Law360, Dec, 6, 2016 (reporting that a tanning salon chain paid $1.5 million to quash claims it violated the BIPA by obtaining customer fingerprints without their consent and failing to properly inform them of how the data would be stored).

194 *See* Kayla Stetzel, Regulations Prevent Some People from Using Google Arts & Culture's Portrait-Matching Feature, Reason, Jan. 24, 2018.

195 *See id.*

196 *See* Aamer Madhani, Treadmill Injuries Send Thousands to the ER Every Year, USA Today, May 4, 2015; *see also* Sabrina Tavernise, Treadmill May Be Riskiest Machine, but Injuries From It Still Rare, N.Y. Times, May 5, 2015.

197 *See Flint v. Strava, Inc.*, No. CGC-12-521659 (Cal. Super. Ct., San Francisco Cnty. June 18, 2012).

198 *See* Helen Pidd, Strava – The App that Turns Cyclists into Racers, The Guardian, July 31, 2013; Frances Dinkelspiel, Parents Sue Cycling Website for Complicity in Son's Death, Berkeleyside, June 19, 2012.

199 *See* Cary Silverman & James Muehlberger, The Food Court: Trends in Food and Beverage Class Action Litigation (U.S. Chamber Inst. for Legal Reform, Feb. 2017).

200 Complaint, *Brickman v. Fitbit, Inc.*, No. 15-cv-2077 (N.D. Cal. filed May 8, 2015).

201 *See* Complaint, *McLellan v. Fitbit Inc.*, No. 3:16-cv-00036 (N.D. Cal. filed Jan. 5, 2016).

202 *See* RJ Vogt, Fitbit Heart-Rate Monitor Row Pushed To Arbitration, Law360, Oct. 12, 2017.

203 *See* Nanci Schanerman, Wearable Technology & Discoverable Data, PropertyCasualty360.com, Oct. 26, 2017.

204 *See Commonwealth v. Risley*, No. CP-36-CR-0002937-2015 (Lancaster Cnty, Pa. initiated Apr. 14, 2015).

205 *See* Dave Altimari, Sister of Connie Dabate Files Wrongful Death Lawsuit Against Richard Dabate, Charged In Murder Case, Hartford Courant, Dec. 19, 2017.

206 *See* Fitbit Privacy Policy, FitBit.

207 *See id.*

208 *See* Decision and Order, *Wisconsin v. Burch*, No. 16CF1309 (Wis. Cir. Ct. Jan. 31, 2018).

209 *See* Laura P. Paton, Sarah E. Wetmore, Clinton T. Magill, How Wearable Fitness Devices Could Impact Personal Injury Litigation in South Carolina, 27 S.C. Law 44 (Jan. 2016).

210 Legal Edge Forum, 3D Printing and the Future of Manufacturing 2 (2012).

211 Alexis Kramer, 3-D Printing Leaps Ahead of Product Liability Law, Bloomberg BNA, Sept. 28, 2016.

212 Michael Weinberg, It Will be Awesome if They Don't Screw it Up: 3D Printing, Intellectual Property, and the Fight Over the Next Great Disruptive Technology, Public Knowledge (Nov. 2010).

213 Michael O. Schroeder, Could 3-D Printing Enhance Your Joint Replacement Surgery?, U.S. News, Apr. 13, 2017.

214 James M. Beck & Mathew D. Jacobson, 3D Printing: What Could Happen to Products Liability When Users (and Everyone Else in Between) Become Manufacturers, 18 Minn. J.L. Sci. & Tech. 143, 150 (2017).

215 Weinberg, *supra*.

216 *Id.*

217 The 10 Best Budget 3D Printers Under $300 in 2018, Aniwaa (last visited Feb. 20, 2018).

218 Sean Rohringer, Large 3D Printers – World's 35 Biggest and Most Expensive, All3P, Oct. 22, 2017.

219 AM Staff, Wohlers Report 2017 Indicates New Business Activity in 3D Printing, Additive Manufacturing (Apr. 12, 2017) (citing the 2017 Wohlers Report, 22nd ed.).

220 TJ McCue, RAPID + TCT 2017 Event to Demonstrate $6 Billion 3D Industry Strength, Forbes, May 2, 2017.

221 Marine Core-Baillais et al., The State of 3D Printing, Sculpteo (3d ed. 2017).

222 *Id.*

223 James M. Beck & Mathew D. Jacobson, 3D Printing: What Could Happen to Products Liability When Users (and Everyone Else in Between) Become Manufacturers, 18 Minn. J.L. Sci. & Tech. 143, 150 (2017).

224 Lucas S. Osborn, Regulating Three-Dimensional Printing: The Converging Worlds of Bits and Atoms, 51 San Diego L. Rev. 553, 555 (2014).

225 Colin Kelly & Jenny Mendelsohn, 3-D Printing Meets Strict Liability in the Auto Industry, Law360, Dec. 8, 2014.

226 Legal Edge Forum, 3D Printing and the Future of Manufacturing 4 (2012).

227 Ford, Press Release, Ford Tests Large-Scale 3D Printing With Light-Weighting and Personalization in Mind, Mar. 6, 2017; *see also* Aaron Smith, Ford is Trying 3D Printing for Car Parts, CNN Money, Mar. 6, 2017.

228 *See* Hayley Lind, Volkswagen Sees a Future in 3D Printing Car Parts, The Drive, Nov. 24, 2017.

229 *See* Stephen Edelstein, Daimler Starts 3D Printing Metal Replacement Parts for Older Mercedes-Benz Trucks, Digital Trends, Aug. 4, 2017.

230 Jay Leno, Jay Leno's 3D Printer Replaces Rusty Old Parts, Popular Mechanics, June 7, 2009.

231 Thomas Kellner, An Epiphany of Disruption: GE Additive Chief Explains How 3D Printing Will Upend Manufacturing, GE Reports, Nov. 13, 2017.

232 *Id.*

233 *Id.*

234 *Id.*

235 *Id.*

236 *See id.*

237 GE Reports Staff, 5 Ways GE is Changing the World with 3D Printing, GE Reports, Aug. 26, 2017.

238 U.S. Food & Drug Admin., Press Release, Statement by FDA Commissioner Scott Gottlieb, M.D., on FDA Ushering in New Era of 3D Printing of Medical Products; Provides Guidance to Manufacturers of Medical Devices, Dec. 4, 2017.

239 Ariel M. Nissan, Regulating the Three-Dimensional Future: How the FDA Should Structure a Regulatory Mechanism for Additive Manufacturing (3D Printing), 22 B.U. J. Sci. & Tech. L. 267, 279 (2016).

240 *See id.*

241 Scott J. Grunewald, Liability and Legal Issues May Derail the Future of 3D Printed Medication, 3D Print.com, Nov. 13, 2015.

242 Melissa Little & Gordon Wallace, Printing the Future: 3D Bioprinters and Their Uses, Australian Academy of Science (last visited Feb. 2, 2018).

243 W. Peng et al., 3D Bioprinting for Drug Discovery and Development in Pharmaceutics, Acta Biomaterialia (May 2017).

244 Tim Lewis, Could 3D Printing Solve the Organ Transplant Shortage?, The Guardian, July 30, 2017.

245 Restatement (Third) of Torts: Prod. Liab. § 19.

246 Beck & Jacobson, 18 Minn. J.L. Sci. & Tech. at 163-64.

247 *See, e.g.*, *Sanders v. Acclaim Entm't, Inc.*, 188 F. Supp. 2d 1264, 1277-79 (D. Colo. 2002) (finding "intangible thoughts, ideas, and expressive content" in videogames are not "products" subject to strict liability law); *K-Mart Corp. v. Midcon Realty Grp. of Conn., Ltd.*, 489 F. Supp. 813, 817 (D. Conn. 1980) (holding that even assuming architect's working drawings, plans and specifications for retail store were "products," they were not subject to product liability law because that "product" substantially changed when transformed from designs drawn on paper into an actual building).

248 Beck & Jacobson, 18 Minn. J.L. Sci. & Tech. at 169; *see also* Shen Wang, When Classical Doctrines of Products Liability Encounter 3D Printing: New Challenges in the Legal Landscape, 16 Hous. Bus. Tax. L. J. 104 (2016).

249 Restatement (Third) of Torts: Prods. Liab. § 1 (emphasis added); *see also* Restatement (Second) of Torts § 402A ("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 there caused.").

250 See Restatement (Third) of Torts: Prod. Liab. § 1 cmt. c; *see also* Lucas S. Osborn, Regulating Three-Dimensional Printing: The Converging Worlds of Bits and Atoms, 51 San Diego L. Rev. 553, 569 (2014).

251 Beck & Jacobson, 18 Minn. J.L. Sci. & Tech. at 156.

252 *See id.* at 157.

253 *See id.* at 152.

254 Lucas S. Osborn, Regulating Three-Dimensional Printing: The Converging Worlds of Bits and Atoms, 51 San Diego L. Rev. 553, 565 (2014).

255 *In re New York City Asbestos Litig.* (Holdampf v. A.C. & S., Inc.), 840 N.E.2d 115, 119 (N.Y. 2005) (quoting *Hamilton v. Beretta U.S.A. Corp.*, 750 N.E.2d 1055, 1060 (N.Y. 2001)) (internal quotations omitted).

256 James M. Beck & Mathew D. Jacobson, 3D Printing: What Could Happen to Products Liability When Users (and Everyone Else in Between) Become Manufacturers, 18 Minn. J.L. Sci. & Tech. 143, 178 (2017).

257 *See generally* Victor E. Schwartz, Phil Goldberg & Christopher E. Appel, Deep Pocket Jurisprudence: Where Tort Law Should Draw the Line, 70 Okla. L. Rev. 359 (2017).

258 *See T.H. v. Novartis Pharm. Corp.*, 407 P.3d 18 (Cal. 2017). The vast majority of courts have rejected this form of "innovator liability," which is premised on the generic drug manufacturer's obligation under federal to convey the same warnings as the U.S. Food and Drug Administrative approved for the brand-name drug. *See* Schwartz, 70 Okla. L. Rev. at 360-69.

259 *See Lawson v. Honeywell Int'l, Inc.*, 75 So. 3d 1024 (Miss. 2011).

260 Scott J. Grunewald, Liability and Legal Issues May Derail the Future of 3D Printed Medication, 3DPrint (Nov. 13, 2015).

261 Beck & Jacobson, 18 Minn. J.L. Sci. & Tech. at 199.

262 *See id.*

263 *Buckley v. Align Tech., Inc.*, 2015 WL 5698751 (N.D. Cal. Sept. 29, 2015).

264 *See id.* at *1.

265 *See id.* at *10.

266 Joseph G. Falcone et al., 3D Printing and Product Liability in the U.S. and UK, Law Journal Newsletters (Oct. 2016).

267 Beck & Jacobson, 18 Minn. J.L. Sci. & Tech. at 187.

268 Technical Considerations for Additive Manufactured Medical Devices: Guidance for Industry and Food and Drug Administration Staff (Dec. 5, 2017).

269 *Id.* at 2.

270 *Id.*

271 *Id.* at 4.

272 U.S. Food & Drug Admin., Press Release, Statement by FDA Commissioner Scott Gottlieb, M.D., on FDA Ushering in New Era of 3D Printing of Medical Products; Provides Guidance to Manufacturers of Medical Devices, Dec. 4, 2017.

273 U.S. Consumer Product Safety Comm'n, Staff Report, Potential Hazards Associated with Emerging and Future Technologies 4 (Jan. 18, 2017).

274 *Id.* at 4.

275 *See* Ryan Randazzo, Uber Reaches Settlement with Family of Woman Killed by Self-Driving Car, The Republic, Mar. 29, 2018; Faiz Siddiqui, Uber Reaches Settlement with Family of Victim Killed After Being Struck by One of Its Self-Driving Vehicles, Wash. Post, Mar. 29, 2018

276 *See* Complaint, *Nilsson v. General Motors LLC*, No 4.18-cv-00471-KAW (N.D. of Cal. filed Jan. 22, 2018).

277 *See* Ethan Baron, Blame Game: Self-driving Car Crash Highlights Tricky Legal Question, Mercury News, Jan. 23, 2018.

278 *See* Complaint, *Nilsson v. General Motors LLC*, at 2.

279 *Id.* at 3.

280 *See* State of California DMV, Report of Traffic Accident Involving Autonomous Vehicle, Dec. 14, 2017.

281 *See* Baron, *supra*; *see also* Peter Holley, After Crash, Injured Motorcyclist Accuses Robot-driven Vehicle of 'Negligent Driving', Wash. Post. Jan. 25, 2018; Rachel Graf, GM Hit With First-Known Suit Over Self-Driving Car Crash, Law360, Jan. 24, 2018.

282 Baron, *supra*.

283 *See id.*

284 Complaint, *Nilsson v. General Motors LLC*, at 5.

285 *See* Nat'l Highway Transp. Safety Admin., Automated Driving Systems: A Vision for Safety 2.0 (Sept. 2017).

286 The priority safety elements include: (1) system safety, (2) operational design domain, (3) object and event detection and response, (4) fallback (minimal risk condition), (5) validation methods, (6) human machine interface, (7) vehicle cybersecurity, (8) crashworthiness, (9) post-crash ADS behavior, (10) data recording, (11) consumer education and training, and (12) federal, state and local laws coordination. *See id.*

287 *See* David Shepardson, U.S. Transportation Agency Calls March 1 'Summit' on Autonomous Cars, Reuters, Feb. 9, 2018.

288 *See* Nat'l Highway Transp. Safety Admin., USDOT Automated Vehicles Activities, Feb. 13, 2018.

289 *See* The Safely Ensuring Lives Future Development and Research in Vehicle Evolution (SELF DRIVE) Act, H.R. 3388, 115th Cong. (2017-2018). The House approved the bill on a voice vote.

290 *See* The American Vision for Safer Transportation through Advancement of Revolutionary Technologies (AV START) Act, S. 1885, 115th Cong. (2017-2018).

291 *See* Nat'l Conference of State Legislatures, Autonomous Vehicles, Self-Driving Vehicles Enacted Legislation, Jan. 2, 2018.

292 States that have enacted autonomous vehicle laws include Alabama, Arkansas, California, Colorado, Connecticut, Florida, Georgia, Illinois, Louisiana, Michigan, Nevada New York, North Carolina, North Dakota, Pennsylvania, South Carolina, Tennessee, Texas, Utah, Virginia, and Vermont.

293 Governors have signed executive orders regarding autonomous vehicles in Arizona, Delaware, Hawaii, Massachusetts, Washington, and Wisconsin.

294 *See* Sharon Jayson, Driverless Vehicles Hit the Road in Texas, U.S. News, Feb. 21, 2018; Cheryl Miller, We Asked California Lawyers for Views on the New Driverless Rules. Here's What They Said, The Recorder, Oct. 13, 2017; Russ Mitchell, Totally Driverless Cars Could be Allowed on California Roads by June 2018, L.A. Times, Oct. 11, 2017.

295 *See* State of Cal. Dep't of Motor Vehicles, Press Release, Driverless Testing and Public Use Rules for Autonomous Vehicles Approved, Feb. 26, 2018.

296 *See* State of Cal. Dep't of Motor Vehicles, Permit Holders.

297 *See* Uniform Law Commission, Press Release, New ULC Committees to be Appointed, Jan. 20, 2017.

298 *See* Nat'l Conference of Commissioners on Uniform State Laws, Draft Tort Law Relating to Drones Act, Mar. 6, 2018.

299 *Id.* § 102(a)(5) (defining "immediate reaches" as 100 feet, but bracketing such text as subject to modification based on state policy preferences).

300 *Id.* § 501, comment (citing Restatement (Second) of Torts § 159(2)).

301 *See id.* §§ 502, 503.

302 *See* Nat'l Conference of State Legislatures, Current Unmanned Aircraft State Law Landscape, Feb. 2, 2018.

303 *See Singer v. City of Newton*, No. 1:17-cv-10071-WGY, 2017 WL 4176477, at *5 (D. Mass. Sept. 21, 2017).

304 *Id.*

305 *See* Dep't of Trans., Presidential Memorandum for the Secretary of Transportation, Unmanned Aircraft Systems Integration Pilot Program, Oct. 21, 2017; Dep't of Trans., Press Release, President Donald Trump and Secretary Elaine L. Chao Announce Innovative Drone Integration Pilot Program, Oct. 25, 2017.

306 *See* Kyle Daly & Shaun Courtney, Chao Doubles Down on Drown, Regulatory Reductions, Bloomberg BNA, Jan. 22, 2018.

307 *See* Bart Jansen, Why it's a Big Deal that Commercial Drones Flew Around the Atlanta Airport, USA Today, Feb. 14, 2017.

308 *See* Fed. Aviation Admin., Press Release, FAA Releases UAS Remote Tracking & ID ARC Report, Dec. 19, 2017.

309 *See* UAS Identification and Tracking (UAS ID) Aviation Rulemaking Committee (ARC), ARC Recommendations Final Report, Sept. 30, 2017.

310 *See Taylor v. Huerta*, 856 F.3d 1089 (D.C. Cir. 2017).

311 National Defense Authorization Act for Fiscal Year 2018, Pub. L. No: 115-91, § 1092(d) (enacted Dec. 12, 2017).

312 Dave Williams, Gov. Deal Signs Spaceport Bill, Atlanta Bus. Chron., May 8, 2017.

313 H.B. 1 (Ga. 2017) (to be codified at Ga. Code Ann. §§ 51-3-41 to -44).

314 Reviving the National Space Council, Exec. Order No. 13803, 82 Fed. Reg. 31,429 (July 7, 2017) (signed June 30, 2017).

315 See Marcia Dunn, Vice President Wants US Businesses Trailblazing Into Space, Wash. Post, Feb. 21, 2018.

316 *See* Loren Grush, How the Trump Administration Wants to Make it Easier for Commercial Space Companies to Do Business, Feb. 23, 2018.

317 National Aeronautics and Space Administration Transition Authorization Act of 2017, Pub. L. No. 115-10 (enacted Mar. 21, 2017); *see also* Dave Mosher, Trump Just Signed a Law that Maps Out NASA's Long-Term Future — But a Critical Element is Missing, Business Insider, Mar. 21, 2017; Derek Richardson, Trump Signs NASA Transition Authorization Act of 2017, Space Insider, Mar. 21, 2017.

318 *See* The American Space Commerce Free Enterprise Act, H.R. 2809, 115th Cong. (2017-2018).

319 *See* Committee on Science, Space & Technology, Press Release, Smith Introduces American Space Commerce Free Enterprise Act of 2017, June 7, 2017.

320 *See* Fed. Trade Comm'n, Press Release, Uber Settles FTC Allegations that It Made Deceptive Privacy and Data Security Claims, Aug. 15, 2017; Sophia Morris, Uber Settles With FTC Over Privacy Misrepresentations, Law360, Aug. 15, 2017.

321 *See* Complaint, *In the Matter of Uber Tech., Inc.*, FTC File No. 152 3054.

322 *See* Decision, *In the Matter of Uber Tech., Inc.*, FTC File No. 152 3054; *see also* Agreement Containing Consent Order, *In the Matter of Uber Tech., Inc.*, FTC File No. 152 3054.

323 *See* Autonomous Vehicles are Just Around the Corner, The Economist, Mar. 1, 2018.

324 *See* Sara Maslin and James Barron, Relief and Trepidation as Ride Hailing Spreads Across New York, N.Y. Times, July 3, 2017; Assoc. Press, Need a Ride? Uber, Lyft Ride-Sharing Apps OK in Upstate NY, US News, June 29, 2017.

325 *See* Joyce Hanson, Hospitality Cases to Watch in 2018, Law360, Jan. 1, 2018 (discussing settlement of litigation over law banning advertisement of short term rentals in New York, legislative proposal in Massachusetts to broaden the state's hotel and motel tax to include short-term rentals, and class action lawsuit by apartment building owners in California to stop Airbnb from allowing their tenants to rent apartments); *see also* Thomas Dickerson, Expert Analysis, A Look at Airbnb's Legal Battles Across the US, Law360, May 9, 2017 (discussing litigation in San Francisco, Santa Monica, Nashville, and New York State).

326 *See* Cara Bayles, Mass. Uber Drivers Can Proceed In Misclassification Row, Law360, Mar. 1, 2018.

327 *See* Cara Bayles, Uber Says Calif. Codes Bar Cab Drivers' Low Pricing Suits, Law360, Jan. 29, 2018; Dorothy Atkins, Uber Must Face Boston Taxicabs' Unlawful Competition Claims, Law360, Jan. 2, 2018.

328 *See* Dorothy Atkins, Uber Drivers' Pay Suit 'Classic' Class Action, Judge Says, Law360, Feb. 8, 2018.

329 *See* Fed. Trade Comm'n, Press Release, FTC Updates COPPA Compliance Plan for Business, June 21, 2017; *see also* Fed. Trade Comm'n, Guidance, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, June 21, 2017.

330 *See id.*

331 *See* Fed. Trade Comm'n, Press Release, FTC Provides Additional Guidance on COPPA and Voice Recordings, Oct. 23, 2017.

332 *See* Behnam Dayanim et al., Key Takeaways From FTC's VTech Privacy Enforcement, Law360, Jan. 18, 2018.

333 *See* Fed. Trade Comm'n, Press Release, Electronic Toy Maker VTech Settles FTC Allegations that it Violated Children's Privacy Law and the FTC Act, Jan. 8, 2018.

334 *See id.*

335 *See* Complaint, *Fed. Trade Comm'n v. D-Link Sys., Inc.*, 2017 WL 65168 (N.D. Cal. Jan. 5, 2017).

336 *See Fed. Trade Comm'n v. D-Link Sys., Inc.*, 2017 WL 4150873 (N.D. Cal. Sept. 19, 2017).

337 *See* Complaint, *Cahen v. Toyota Motor Corp.*, No. 3:15-cv-01104 (N.D. Cal. filed Mar. 10, 2015).

338 *See Cahen v. Toyota Motor Corp.,* 147 F. Supp.3d 955 (N.D. Cal. 2015).

339 *See Cahen v. Toyota Motor Corp.,* 2017 WL 6525501 (9th Cir. Dec. 21, 2017).

340 *See* Complaint, *Flynn v. FCA US LLC*., No. 3:15-cv-0855 (S.D. Ill. filed Aug. 4, 2015).

341 *See Flynn v. FCA US LLC*, No. 15-cv-0855, 2017 WL 3592040 (S.D. Ill. Aug. 21, 2017).

342 *See* Dave Simpson, Hacking Suit Should Be Tossed, Fiat Chrysler Tells Judge, Law360, Jan. 19, 2018.

343 *See* Motion for Reconsideration, *Flynn v. FCA US LLC*, No. 3:15-cv-0855 (S.D. Ill. filed Jan. 18, 2018).

344 *See* Simpson, Hacking Suit Should Be Tossed, Fiat Chrysler Tells Judge, *supra*.

345 SPY Car Act of 2017, S. 680, 115th Cong. (2017-2018).

346 DIGIT Act, S. 88, 115th Cong. (2017-2018); H.R. 686, 115th Cong. (2017-2018).

347 Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S. 1691, 115th Cong. (2017-2018).

348 *See* generally Dirk A. Zetzsche et. al., Regulating A Revolution: From Regulatory Sandboxes to Smart Regulation, 23 Fordham J. Corp. & Fin. L. 31 (2017).

349 *See, e.g.*, John Frank Weaver, Robots Are People, Too, Slate, July 27, 2014.

Notes

U.S. CHAMBER
Institute for Legal Reform

202.463.5724 main
202.463.5302 fax

1615 H Street, NW
Washington, DC 20062

instituteforlegalreform.com