U.S. CHAMBER
Institute for Legal Reform

Torts of the Future

Addressing the Liability and Regulatory Implications of Emerging Technologies

MARCH 2017

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, Phil Goldberg & Jonathan Wilson[†], Shook, Hardy & Bacon L.L.P.

Executive Summary

Emerging technologies are changing how we live, travel, and buy goods and services. If the pace of this transformation continues as expected, in 2025 it may be common for a refrigerator to reorder our food and a drone to deliver it, while a driverless car takes us to the spaceport for a flight into low-earth orbit. 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?

While there are many emerging technologies worthy of consideration, this report closely considers five areas:

1. Autonomous vehicles;
2. Commercial use of drones;
3. Private space exploration;
4. The "sharing economy," which allows people to generate income from underused assets, such as cars and rooms; and
5. The Internet of Things, which involves products that are connected to collect and share data.

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?
- Will courts alter these principles to expand liability?
- Is there significant potential for overregulation by Congress, state and local governments, and government agencies?
- How might regulation and liability interact?

- Is there adequate insurance coverage available?
- Is there a need to place constraints on liability?

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

Autonomous Vehicles

Experts predict that fully autonomous vehicles will be widely available by 2025. Cars that drive themselves and communicate with each other and infrastructure are expected to eliminate human error, saving thousands of lives each year. But some accidents will undoubtedly continue to happen, including as a result of people who continue to drive themselves, failures in the human-car interaction, or decision-making errors by the car.

When an accident occurs, who will be responsible for compensating those who are injured? Will car accidents routinely result in product liability lawsuits against automakers, rather than the typical negligence or fault-based approach that currently exists between drivers? If so, how would that liability be balanced against the thousands of people who each year are no longer killed on the roadways because of that technology? How will these changes alter the responsibility of people and manufacturers to have insurance? Will these changes require a new liability framework?

Plaintiffs' lawyers have suggested imposing strict liability on manufacturers for any car accident involving an autonomous vehicle. Others are considering alternatives to traditional tort liability, such as no-fault insurance or an accident victim compensation fund, to make sure that excessive liability does not improperly chill this promising technology and the huge advances in overall public safety it promises. Legislatures and courts should consider all of these issues to ensure that the liability framework around this technology advances sound public policy.

Commercial Use of Drones

Small unmanned aircraft systems, also known as drones, are already used in industries ranging from agriculture to real estate. As a result of new FAA regulations that make it easier for businesses to operate drones, commercial drone sales are expected to surge from a few thousand to millions per year. However, continued restrictions on flying drones over people and beyond an operator's line of sight keep drones unavailable for many uses, such as delivering products. Efforts are underway to reduce these constraints, even as some state and local governments adopt their own restrictions.

At this point, there is little drone-related litigation. As drones come into routine use, however, there will inevitably be instances in which they collide with people or property, distract drivers, or capture images or video of people on private property. Such encounters will likely result in product liability claims against drone makers, and negligence, trespass, nuisance, and invasion of privacy claims against the businesses that operate them. In most cases, traditional principles of tort law, potentially guided by FAA regulations that may inform the standard of care, should sufficiently address claims that arise.

Drone use may require courts to address long unresolved legal issues, such as where private property ends and the public airspace begins. Courts will also consider whether a drone is defective if it does

not include the most sophisticated safety technology, which could make drones prohibitively expensive. Some states have adopted drone-specific privacy laws, including a private right of action, which will lead to novel claims.

The extent of liability exposure could cause businesses that have developed technology to deliver packages, pizzas, or even burritos by drone to rethink their plans.

Private Space Exploration

Over the past three decades, the United States has increasingly relied on private companies for its space program. These companies are already developing and testing vehicles that will take space tourists to low-earth orbit and even to the moon. Other firms are developing technology to gather resources from asteroids to make fuel, which could make deep space exploration possible. While offering incredible opportunities, these activities also have significant inherent risks. Private space exploration, as with historically government-led missions, could have tragic results.

International law governing liability for damages that occur as a result of space activities dates back to before the first moon landing. Meanwhile, Congress has passed a series of laws to encourage growth of commercial space activity, adopt a shared approach to liability, and provide a "learning period," precluding government regulation of commercial spaceflights until 2023, unless an actual experience warrants action. In addition, at least seven states have enacted laws designed to attract companies to locate spaceflight operations in their states. These laws generally require private operators to inform spaceflight participants of the inherent risks and limit the operators' liability.

This balanced approach to regulation and liability policy has facilitated a thriving commercial space industry. To continue this progress, regulators should promote development of voluntary industry consensus standards for commercial spaceflights. When an incident inevitably occurs, they should resist the urge to impose heavy-handed regulations that go beyond addressing an identified problem. Without reasonable constraints on liability, a single failure could place the commercial space industry, and companies that insure their operations, into a tailspin.

The Sharing Economy

People have long bartered for goods and services, but the internet and spread of mobile devices has vastly expanded the pool of potential sellers and consumers. Companies have now developed platforms that facilitate these transactions and create the trust needed for exchanges between complete strangers. This is known as the sharing economy. Ride-sharing and home-sharing services are among the best known and rapidly growing examples, but companies have already developed over 10,000 new platforms that facilitate everything from dog walking to providing medical services.

The sharing economy comes with its own set of liability risks that can jeopardize its viability. For example, companies that provide ride-sharing platforms face litigation over whether drivers are independent contractors or employees. If courts view these companies as employers, they will be exposed to wage-and-hour litigation and could be held liable when a driver gets into an accident.

The sharing economy can also be crushed by unnecessary regulation. These types of businesses have rapidly grown

precisely because entry barriers are low and existing restrictions have resulted in unmet consumer needs. Before imposing burdensome or ill-fitting regulations, policymakers should evaluate whether current safeguards adopted by the companies, such as background checks, insurance requirements, two-way rating systems, and complaint resolution centers, address concerns.

The Internet of Things

Many everyday items are embedded with technology allowing them to collect and share information—from televisions to baby monitors. This is known as the "Internet of Things" (IoT). It will not be long before devices connected to the internet are as common as those connected to an electrical outlet. This new connected world provides consumers and businesses with significant benefits, but also poses liability risks.

There is already litigation targeting connected products. Automakers, a medical device manufacturer, and children's toymakers have faced lawsuits claiming that their products *could be* maliciously hacked or used to spy on consumers.

More of these types of lawsuits can be expected in the future, and courts may be tempted to relax traditional requirements, such as the need for a plaintiff to have standing to sue by showing an actual injury, not fear of a future harm. Courts may also reexamine tort law principles that limit a business's liability for the criminal acts of third parties, evaluate whether a product is defective at the time of sale, and severely limit post-sale duties to warn consumers of product risks. If courts expand liability, manufacturers of connected products could find themselves exposed to a continuing obligation to monitor and patch vulnerabilities for the life of the product.

Regulators are beginning to weigh in. While there are no IoT-specific laws or regulations, five federal agencies recently published guidance addressing how manufacturers should incorporate security into connected devices. Courts may look to these guidelines, as well as industry practices, to evaluate whether a manufacturer met the standard of care in developing a connected device.

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 that promotes innovation and entrepreneurship, while addressing legitimate safety and privacy concerns. To achieve this goal, this report offers eleven "guiding principles" for the consideration of courts and policymakers.

Autonomous Vehicles

Researchers estimate that autonomous vehicles can reduce accident rates by up to 90%,[1] which would save over 30,000 lives each year[2] and avoid millions of injuries on American roads. As General Motors Chairman Bob Lutz said, "The autonomous car doesn't drink, doesn't do drugs, doesn't text while driving, and doesn't get road rage. Autonomous cars don't race other autonomous cars, and they don't go to sleep."[3] But technology is not perfect. Though people may be much safer in a driverless car than a traditional vehicle, it is still likely that accidents will occasionally occur due to a failure in technology, the human driver-car interface, maintenance, or other factors. There is a vigorous debate over how to fairly apportion liability in these situations without chilling life-saving technology.

The human health and safety benefits of autonomous vehicles (AVs), also known as driverless cars, are broadly hailed. A 2013 study by the Eno Center for Transportation found that if only 10% of the cars on the road were self-driving, 1,000 lives and $18 billion would be saved each year.[4] When 90% of the cars are autonomous, those numbers jump to 22,000 lives and $350 billion.[5] In a widely cited study on the auto insurance industry, audit company KPMG found that autonomous technology will reduce accident frequency by 80% by 2040.[6]

In addition, driverless cars are expected to have broader societal benefits, including easing traffic congestion, moving people to destinations more quickly, burning less fuel, and lowering emissions.[7] They also can provide mobility to seniors, people with vision problems, and others who cannot drive on their own.[8] It is widely expected that cities will be stocked with fleets of shared driverless cars and that people who spend long stretches of time on the road will be able to do so more efficiently. In short, driverless cars promise to fundamentally change the way people get around. Auto travel will be significantly safer with benefits that ripple throughout society.

The National Highway Transportation and Safety Administration (NHTSA), in an effort to facilitate the advancement and development of automated car technology,

> *In short, driverless cars promise to fundamentally change the way people get around. Auto travel will be significantly safer with benefits that ripple throughout society.*

issued the Federal Automated Vehicles Policy in September 2016. The guidance, titled "Accelerating the Next Revolution in Roadway Safety,"[9] recognizes that autonomous car technology will be introduced in stages. Already, many features, such as front-end collision, lane assist and modified cruise control, are having an impact. To assist the progression toward fully autonomous cars, NHTSA provides a framework for data sharing, privacy and cyber security, ethics, and other issues likely to arise in the next few years.

> *NHTSA guidance advises states to consider how to appropriately allocate liability among automated vehicle owners, operators, passengers, manufacturers, and others.*

NHTSA's report identifies liability—and the resulting insurance implications for consumers and manufacturers—as a major issue that needs to be addressed. However, it recognizes that, at least to this point, liability and insurance issues have largely been left to the states under a patchwork of negligence, product liability, and insurance laws. NHTSA guidance advises states to consider how to appropriately allocate liability among automated vehicle owners, operators, passengers, manufacturers, and others.[10] The agency suggests that, given the complexity of these issues and the need for a certain level of uniformity, "[i]t may be desirable to create a commission to study liability and insurance issues and make recommendations to states."[11]

Autonomous Car Technology

When people refer to autonomous cars, they are largely referring to technology that exists within each car that allows the car to read its surroundings and make driving decisions based on those readings. The Society of Automobile Engineers (SAE International) has developed a taxonomy and definitions for terms related to these systems that have become widely used. SAE identified six automation levels, from Level 0 (no automation) to Level 5 (full automation).[12]

A key distinction exists between SAE's Levels 2 and 3. Level 2 is called "partial automation," and the human driver remains responsible for monitoring the environment and performing key driving tasks. When a car reaches Level 3 automation, which SAE calls "conditional automation," the automated car performs all of the dynamic driving tasks, with the human driver acting as the fallback option.

As indicated, cars operating at Level 3 are equipped with computer mapping systems, radar, cameras, sensors and other technologies that allow them to read their

environment, including the shape of the roads, traffic and driving conditions, and perform key dynamic driving tasks. Yet, these cars are not fully automated. They ultimately require human control and may have features, such as steering wheel sensors, to require the human driver to stay alert and engaged. It is anticipated that the automated features may work only when the driver's hands are on the wheel because the system anticipates the driver will take control of the car in certain situations.

Highly automated vehicles (Level 4), which in most environments are fully autonomous, are anticipated to be widely available by 2025.[13] Between 2025 and 2040, experts expect that vehicles will move towards Level 5—a "new normal" of integrated driving in which there is communication between vehicles and infrastructure and vehicles can operate without any driver present.[14]

Vehicle-to-vehicle communication (V2V) will rely on short-range radio devices to transmit vehicle speed, direction, braking and other key data points between vehicles. The benefit of this technology is that it will allow a car to "see" around corners and through traffic so that it can better anticipate when it needs to brake and avoid potential collisions. In early stages of automation, this information can be given to human drivers to make their own decisions. NHTSA, which is developing standards for V2V communication, estimates that this technology can eliminate 81% of all crashes.[15]

Congress has also funded NHTSA's research into vehicle-to-infrastructure communication (V2I) networks, whereby cars receive data from roadways and traffic lights. Such data may include bad weather conditions, the shape of the road and whether there are any steep curves ahead, the nature of any construction zones, and when lights are about to turn red. Rather than accelerate through a yellow light, as many humans do, the car could anticipate the red light sooner and slow down more safely and comfortably.

The greatest safety gains will be made when all three of these technologies work together.

The Race to Autonomous Driving

About 20 companies are developing self-driving cars, including traditional auto manufacturers, technology companies, and ride-sharing services.[16] Several of them have test cars on the road and are collecting data on the ability of the cars to properly read the environment and make the right driving decisions. Humans can repeat mistakes over and over again, but the goal for automated cars is to be programmed to learn from and not repeat mistakes. To this end, NHTSA is working on a data-sharing program, which it hopes to have in place by the end of 2017, so that companies can learn from each other and accelerate the elimination of errors.

Among the more well-known self-driving features is Tesla's "autopilot" technology, which is intended to guide drivers on highways. In May 2016, a driver was killed when he reportedly relied entirely on the autopilot system to drive his Model S, which was not its intended use.[17] The car crashed into the side of a truck that was crossing the highway. Tesla found that the autopilot did not recognize "the white side of the tractor against a brightly lit sky."[18] In January 2017, NHTSA completed its investigation, concluding that there was no defect in the design or performance of Tesla's autopilot system.[19] The agency recognized that since autopilot is not cross-traffic aware, it requires a driver's "continual

and full attention to monitor the traffic environment," and the driver had sufficient time to brake to avoid the accident.[20]

> *"In January 2017, NHTSA completed its investigation, concluding that there was no defect in the design or performance of Tesla's autopilot system."*

Nevertheless, the incident has been a touchpoint for liability discussions. Was the driver to blame for not being attentive? Does Tesla have liability because the car did not stop on its own? Or is responsibility shared? If shared, then how is that responsibility divided?

Google has also received significant attention for its autonomous car program, which is not yet available to the public. Google first retrofitted existing cars with its driverless technology, but has since developed its own "bubble car." Collectively, Google's cars have more than two million miles of driving data.[21] Google's vision is to have no steering wheels, brakes or any other human controls to avoid confusion in the human-car interface.

A minor accident occurred when a Google car, which had a human engineer inside, was negotiating merging traffic. Both the car and the engineer thought a bus would let them in, but the bus continued and the Google car sideswiped the bus.[22] No one was injured in the February 2016 collision.

The ride-sharing service Uber began test-driving its autonomous cars in Pittsburgh in September 2016. Consumers have the option to choose an autonomous car, which has a driver ready to take control along with an engineer in the passenger seat. The Pennsylvania Insurance Department is treating the cars' self-driving features in the same way it treats cruise control, meaning the human driver is fully responsible for accidents under a negligence standard. Uber announced that it has $1 million in third-party liability insurance and $5 million in total coverage per incident.[23]

California took a different approach, requiring a special permit for autonomous cars and instructing Uber to stop its self-driving car service in San Francisco until it did so.[24] Uber took the position that its cars did not need the permit because each car had a driver behind the wheel, ready to take control. The state then revoked the registration of 16 Uber-owned vehicles in December 2016.[25] Uber's San Francisco program lasted only a week before the company loaded its vehicles on a flatbed and moved them to Arizona.[26] Arizona Governor Doug Ducey welcomed the program with "open arms and wide open roads."[27]

Major auto manufacturers, which have been incorporating elements of self-driving technology into cars, are also heavily investing in research and development toward fully autonomous vehicles. In February 2017, Ford announced plans to invest $1 billion over the next five years in start-up company Argo AI, with a goal of producing self-driving cars for ride-sharing services by 2021.[28] General Motors made a similar investment in Cruise Automation and the ride services company Lyft. It

is anticipated that ride-sharing services such as Uber and Lyft will be the way that most people will be introduced to autonomous vehicles.

The Vigorous Debate Over the Liability Framework for Injuries Involving Autonomous Vehicles

While heavy-handed regulation can quickly drive out autonomous vehicles, the area with the greatest potential "to derail this important technology" is excessive litigation.[29] Outsized liability, particularly in the early development and deployment stages, "could seriously undermine this potentially unprecedented public health success story."[30] It "could delay or even wipe out the vision of driverless cars gaining widespread consumer use."[31]

LIABILITY BASED ON A FAILURE IN THE HUMAN-CAR INTERFACE

The immediate question for Congress, state legislatures, and courts to decide is how to treat liability over the next twenty or so years as society transitions to widespread use of fully-automated cars. During this period, humans and cars' self-driving technology will share the roads and responsibility and control over driving decisions. Therefore, as the Brookings Institution's Center for Technology Innovation found in a 2014 study, there will be "complex questions of liability shared by both the human driver and autonomous vehicle technology providers."[32]

Industry experts broadly agree with both the complexity and importance of getting the liability right during this phase-in period. "We're entering a whole new world of assessing who's at fault in an accident and where the ultimate liability and risk ultimately falls," explained Joe Schneider, an insurance analyst with KPMG.[33] David Strickland, a former NHTSA Administrator, echoed this point: "There is going to be a moment in time when there's going to be a crash and it's going to be undetermined who or what was at fault. . . . That's where the difficulty begins."[34]

States are beginning to tackle these liability issues. California and Nevada law explicitly places liability for any accident on the "operator" of the autonomous vehicle, defining the operator as the person behind the controls or who "causes the technology to engage."[35] Under general tort law principles, the element of control is likely to be determinative in other states as well. "Suppose you're in a driverless car, and you see that you're about to rear-end another car. Whether you bear some responsibility for the crash may ultimately turn on the degree of *control* you had over the car. Could you have reasonably prevented the accident, or not?"[36] One question that has arisen is whether this test can be applied fairly when the human "driver" has a disability, such as blindness, and cannot take control.

Other questions also arise: What happens if a driver falls asleep and the vehicle had driver monitoring systems that failed to

"While heavy-handed regulation can quickly drive out autonomous vehicles, the area with the greatest potential 'to derail this important technology' is excessive litigation."

wake up the driver? Can a driver legally rely on this feature (or lane or brake assist) and sue the manufacturer when the car did not alert him or her of a hazard? Should the driver be absolved of his or her own negligence? Can a manufacturer be subject to liability for not preventing an accident, even though its technology did not cause the harm?

As a legal matter, complete reliance on such prophylactic safety devices is likely to be seen as unreasonable. It also does not make practical sense to subject manufacturers to liability just because their safety devices were not able to prevent harm in every instance. Even if a preventative safety device avoids harm 20% of the time, it still offers improved safety over vehicles without that technology. Excessive liability for the remainder of the cases could delay their introduction or stop these technologies from being improved over time. If the device did not cause harm, there should be no liability under commonsense and traditional tort principles.

Novel liability issues will arise when accidents occur between human drivers and autonomous cars. For example, there may be differences between how humans and autonomous cars drive.[37] Autonomous cars may be programmed to drive in 100% compliance with the law. They may drive at the speed limit on a highway where the traffic customarily moves significantly faster, come to a full stop and pause at a stop sign, or stop at a yellow light where most drivers would have continued through. People who are unaccustomed to such "safe" driving could rear-end an autonomous vehicle. Finally, when a fender bender involves a human driver and a fully-autonomous vehicle, should the law recognize a presumption that the accident occurred as a result of human error absent a showing of a defect in the autonomous vehicle?

"Novel liability issues will arise when accidents occur between human drivers and autonomous cars."

NEGLIGENCE VS. PRODUCT LIABILITY

Courts will be faced with determining the appropriate standard of care for evaluating whether an autonomous-vehicle manufacturer is subject to liability for a car accident. Traditionally, car accidents are assessed through the lens of driver negligence, with the potential for product liability only when a defect in the car causes the accident or is alleged to have exacerbated the injuries. A manufacturer has never had a duty "to design an accident-proof or fool-proof vehicle."[38]

Legal scholars suggest that negligence should continue governing liability for car accidents, whether due to the decision-making of autonomous vehicles or human drivers. They explain that these situations differ from traditional product harms because of the huge safety gains: "Holding computer-generated torts to a negligence standard will result in an improved outcome; it will accelerate the adoption of automation" and thereby reduce accidents.[39]

A negligence assessment would focus on whether the car's decision or act showed a lack of due care under the circumstances, not whether the computer was improperly designed or marketed.[40] In the accident

between Google's autonomous car and the bus, the inquiry would be whether it was negligent to merge into traffic given the speed of the bus, distance between the bus and car in front of it, and other such factors. The car's programming can then be updated to account for any new information gained as a result of the incident to help the cars make better decisions going forward.

"Personal injury attorneys fearing that their business may dry up with the adoption of driverless cars," however, are looking for ways to pursue "autonomous-vehicle makers and their deep pockets."[41] They want to shift liability away from negligence claims against drivers with liability insurance limits to product liability lawsuits targeting car manufacturers, software designers, and component makers.[42]

To this end, the American Association of Justice (AAJ), the national plaintiffs' lawyer organization, issued a report in February 2017, advocating that manufacturers should bear the burden of car injuries.[43] While AAJ acknowledged the "revolutionary impact" that so-called "robot cars" will have on public safety,[44] it asserted that imposing strict liability on automakers "may eventually be the most appropriate approach to liability."[45] Under AAJ's approach, "manufacturers would accept responsibility for all crashes caused by their cars.[46]

ALTERNATIVE LIABILITY THEORIES

The desire to provide compensation for people injured in autonomous cars without chilling the advancement of this life-saving technology has led legal scholars to consider alternatives to traditional tort liability. Two oft-mentioned options are no-fault insurance and a victim compensation fund. Both have precedent and both can be shaped to address the specific needs of the autonomous vehicle market.

The RAND Corporation found that rather than shift liability from the driver to the auto manufacturer, as AAJ suggests, it would be more beneficial for drivers to carry no-fault liability insurance.[46] A dozen states have used no-fault liability since the 1970s. The benefit of this system is that drivers maintain their own insurance and are compensated up to a certain level regardless of whether anyone, including the driver, was legally at fault. Lessons can be learned from current no-fault systems so that one can be tailored to autonomous cars to maximize efficiency.

Another option is for states or the federal government to establish a fund to compensate those who are injured, much like the National Childhood Vaccine Injury Fund. Congress established the Vaccine Fund in 1986 when liability concerns threatened public health by jeopardizing access to vaccines. Under this system, anyone injured by a vaccine can apply to the Fund for fair compensation without having to establish fault. The trust fund is financed through a nominal ($0.75) excise tax on each dose of vaccine routinely administered to children to prevent disease.[47] As a result of the Fund, immunizations have increased, supplies have remained stable, and prices have decreased. A fund tailored to the autonomous car market could have a comparable effect—assuring that those who are injured in accidents receive compensation while not allowing excessive liability to impede the development and advancement of technology that makes the roads safer for everyone.

Federal preemption of state tort claims in conjunction with either of these no-fault regimes "could speed the development and utilization of this technology and should be considered, if accompanied by a comprehensive federal regulatory regime."[48]

> *"The desire to provide compensation for people injured in autonomous cars without chilling the advancement of this life-saving technology has led legal scholars to consider alternatives to traditional tort liability."*

The Road Forward

Consumers, manufacturers, and insurers need to feel they are treated fairly in the event of a crash. Developing confidence in the safety of autonomous vehicles and the availability of a just remedy should an injury occur is important to gaining acceptance of the new technology.

Understanding this need, some manufacturers have said that they will accept liability for accidents involving their fully-autonomous cars. Erik Coelingh, Volvo's senior technical leader for safety and drive support technologies, explained that when the company's fully-autonomous system debuts as anticipated in 2020, its vehicles will include several redundancies to avoid accidents and eliminate human error: "Whatever system fails, the car should still have the ability to bring itself to a safe stop."[49]

Tesla has stated that it will accept liability if an accident is "endemic to our design."[50] Tesla's Elon Musk said that "point of views on autonomous cars are much like being stuck in an elevator in a building. Does the Otis [Elevator Company] take responsibility for all elevators around the world, no they don't."[51] But they do when an incident is their fault. Tesla has shared information with NHTSA showing that crash rates involving its vehicles dropped nearly 40% since autopilot came online.[52]

In the shortterm, courts will need to work through these thorny issues, and determine and allocate liability, on a case-by-case basis.

Commercial Use of Drones

In August 2016, the Federal Aviation Administration (FAA) significantly lowered restrictions on the commercial use of small unmanned aircraft systems (sUAS), also known as unmanned aerial vehicles (UAVs) or drones.[53] As a result, the agency predicts that the number of drones registered for commercial use will expand from 20,000 prior to the new regulations to 600,000, a 30-fold increase, within one year.[54] By 2020, the FAA predicts 2.7 million commercial drones, in addition to 4.3 million recreational drones, will be sold annually.[55] As drones fill the skies, courts are likely to experience a surge of litigation resulting from accidents and privacy concerns.

Commercial use of drones has been authorized since 2014, but, until recently, restrictive FAA regulations kept them from widespread use. Commercial operators needed to have a manned aircraft pilot's license or obtain special case-by-case authorization from the agency, known as a "Section 333 exemption."[56] Before September 2016, the FAA approved over 5,500 of these exemptions based on individual safety evaluations.[57] (Separate regulations govern use of drones for recreational purposes.) Critics noted that the Section 333 exemption process was "cumbersome, lacked flexibility and often took many months," posing a roadblock to innovation.[58]

Drones already have a variety of commercial uses. They are popular for aerial photography, real estate agents use them to get birds-eye videos of properties, and they are helpful for inspecting and monitoring buildings, cell phone towers, construction sites, and bridges.[59] Ranchers use drones to count cattle.[60] Drones also help farmers with planting and crop rotation strategies.[61] Drones are used by filmmakers, for firefighting, for search-and-rescue work, and for academic research.[62] They can be controlled by smartphone, iPad, or other device.

Businesses that deliver goods are watching, waiting, and planning to take advantage of the technology to serve their customers. Amazon and Google, for example, are developing and testing technology to deliver products purchased online by drone.[63]

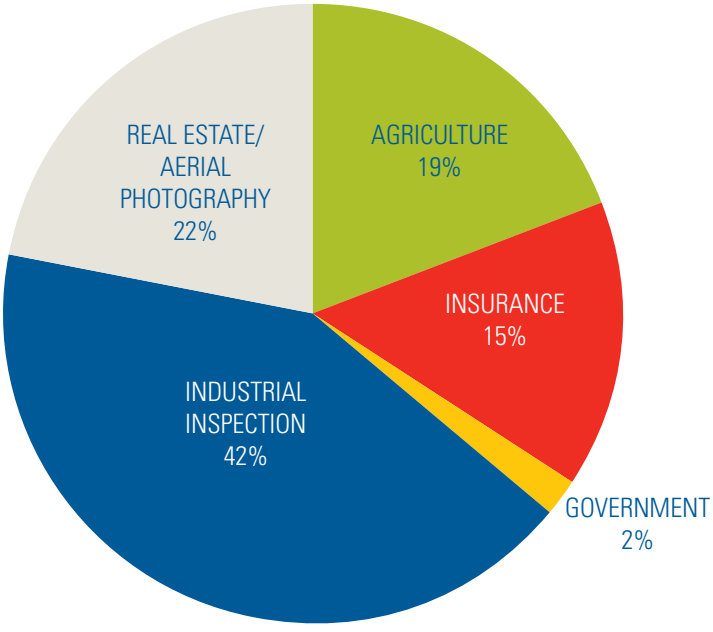
In the northern Russian city of Syktyvkar, Dodo Pizza began deliveries by drone

in 2014.[64] Even before that, however, engineers from Yelp developed a prototype "Burrito Bomber" that drops food via drone with the aid of a parachute to fulfill app-placed customer orders.[65] They planned on starting deliveries in 2015, when they anticipated that the FAA would lift tight restrictions on drone use. They are still waiting to make deliveries by drone.

The New Drone Regulations

The FAA regulations that took effect on August 29, 2016, mark a new era for commercial drone use. They replace the Section 333 exemption process with a rule that broadly allows businesses to use small drones in low-risk scenarios. No longer does a drone operator need to obtain a traditional pilot's license or obtain case-by-case approval from regulators. There is now a new and simpler aviation knowledge exam and background check that results in a two-year remote-pilot certificate.[66]

TOP 5 MARKETS FOR COMMERICAL DRONES



Source: FAA Aerospace Forecast: Fiscal Years 2016-2036, at 33 (2016).

> *"FAA regulations that took effect on August 29, 2016, mark a new era for commercial drone use."*

There continue to be significant limitations on drone use, however. A drone must weigh less than 55 pounds, including any item it is carrying.[67] Flights cannot go beyond the operator's line of sight, be conducted at night, go above 400 feet in the air, or move at speeds faster than 100 miles an hour.[68] All drones must be registered with the FAA. Drone operators can seek a waiver of most of these restrictions, so long as they can show the operation can be conducted safely.[69] The agency encourages applicants to submit a request at least 90 days before the proposed operation.[70] Operators can make a request through quick submission of an online form.[71] The FAA has granted about 320 waivers since August 2016, with all but a handful seeking to operate drones outside of daylight hours.[72] Time will tell whether the waiver process provides the flexibility and speed that commercial operators seek.

By significantly reducing entry barriers and restrictions, the new regulations are likely to lead to an immediate rise in drone use in some industries, such as insurance, construction, and real estate.[73] As a practical matter, however, the line-of-sight requirement and prohibition against flying

over people remain major obstacles for the use of drones in other areas, such as by news organizations, law enforcement, and companies that would like to make deliveries.

Expanded Commercial Use on the Horizon

As noted earlier, the FAA expects that its new regulations will lead to a surge in commercial drone sales over the next three years.[74] The agency anticipates that two categories of small drones will emerge: low-end models, primarily for hobbyist and recreational use, with an average sale price of $2,500; and higher-end models, likely for commercial use, with an average sale price of $40,000.[75] Low-end models are predicted to make up about 90% of the market.[76]

The 2016 regulatory changes, however, are just the first steps in lowering barriers to commercial drone use.

The FAA already has an effort underway to develop a regulatory framework that would allow drones to operate over people not directly involved in the operation of the aircraft in certain conditions.[77] The Aviation Rulemaking Committee (ARC), composed of a diverse range of aviation stakeholders, issued a final report to the FAA on April 1, 2016.[78] The ARC recommended no restrictions for drones that weigh 250 grams or less (about one-half pound). For larger drones, the ARC recommended risk-based standards for flying over people. Drones over 250 grams would be placed into three categories, each with additional restrictions, based on an "impact-energy threshold" and the chance of a serious injury. Though stakeholders anticipated release of the drone-over-people rule in late 2016, the FAA is still considering privacy and safety concerns as it prepares the rule for public comment.[79]

In addition, the FAA established a Drone Advisory Committee (DAC) in July 2016, tasking it with developing consensus-based recommendations for regulatory priorities that "simultaneously promote innovation, safety, efficiency and rapid integration" of drones into U.S. airspace.[80] The group is led by Intel CEO Brian Krzanich. Its 35 members include representatives of the media, airlines, aircraft manufacturers, aircraft pilots and owners associations, airports, traditional delivery companies, academics, Amazon, Google, Garmin, and Facebook.[81] The FAA views the DAC as having an ongoing advisory role.[82]

The FAA has not set a timeline for addressing the use of drones to deliver products.[83] To take this step, the FAA will need to allow drones to fly beyond the operator's visual line of sight. Accomplishing this goal may require technology to reduce the potential for mid-air collisions. NASA is reportedly developing technology that could provide air traffic control for low-flying commercial drone operations.[84] The FAA is also working with other agencies to test technology that would detect unauthorized drones near airports or critical infrastructure.[85] The FAA expects demand "to soar" once it allows drones to fly beyond visual line of sight.[86]

Some businesses would like to see the FAA move more quickly to make expanded commercial use of drones a reality. As FAA Administrator Michael Heurta has acknowledged, "innovation moves at the speed of imagination, [while] government has traditionally moved at, well, the speed of government."[87] Heurta indicated in a speech to stakeholders that the FAA is trying to move faster and maintain a "flexible regulatory approach."[88]

> *"As FAA Administrator Michael Heurta has acknowledged, 'innovation moves at the speed of imagination, [while] government has traditionally moved at, well, the speed of government.'"*

The Potential for Overregulation

Drone makers expect that commercial use of drones will create more than 100,000 jobs and generate more than $82 billion for the economy over the next decade.[89] But overregulation of drone use could impede innovation and pose a barrier to production.

While safety concerns necessitate some degree of federal regulation of drones, there is a danger that state and local government will impose additional layers of regulations that could unnecessarily discourage businesses from using the technology. According to the National Conference of State Legislatures, 38 states considered legislation related to drones in 2016 and 18 states enacted new laws.[90] Several major cities, such as Chicago, Los Angeles, and Miami, have also imposed restrictions in recent years.[91]

Chicago became the first major city to regulate drones in November 2015.[92] Many of the provisions of the ordinance track the FAA regulations, such as prohibiting drones from flying near airports, higher than 400 feet, over people, outside the line of sight of the operator, at night, or when the operator is under the influence of alcohol or drugs.[93] But the ordinance also imposes additional operational restrictions. Absent the owner's consent, the ordinance broadly prohibits flying drones over property the operator does not own, as well as over any school, hospital, place of worship, prison, or police station, or using drones for surveillance purposes.[94] Violators are subject to a fine of between $500 and $5,000, imprisonment for up to 180 days, and seizure of the drone.[95]

Although the Chicago ordinance was adopted before the FAA finalized its new regulations governing small drones, the ordinance appears to carve out operating a drone within the terms of an FAA-approved waiver.[96] Requirements to register drones with the city, attach identification tags, and mandate drone operators to obtain insurance coverage naming the city as an additional insured were dropped from the final ordinance.[97]

The following month, as the FAA continued to develop its new drone regulations, the FAA's Office of the Chief Counsel opined that a "patchwork quilt" of varying restrictions on drone use could jeopardize the agency's efforts. The FAA issued a Fact Sheet, finding that the proposed federal framework preempts certain state and local laws "[t]o ensure the maintenance of a safe and sound air transportation system and of navigable airspace free from inconsistent restrictions."[98] The Fact Sheet provides examples of local regulations that are not permissible without FAA approval, such as those that impose additional registration or training requirements, regulate altitude

> *[Governor Brown] expressed concern that a 'patchwork of federal, state, and local restrictions on airspace' creates 'significant regulatory confusion. Piecemeal is not the way to go.'*

or flight paths, or attempt to ban drones within the airspace of a city.[99] The guidance document takes the position that states and localities may continue to enact laws regarding drone use that are related to traditional state policy powers, such as laws protecting privacy or addressing use of drones by law enforcement.[100] The FAA is on solid legal ground in taking this position, as courts have consistently ruled that federal aviation regulations sufficiently demonstrate Congressional intent to preempt the field of aviation safety.[101]

California Governor Jerry Brown has heeded the FAA's position, vetoing several bills passed by the California General Assembly in 2015 and 2016. These bills would have imposed restrictions on flying drones over property,[102] prohibited drones from flying over parkland,[103] and required drone makers to outfit products with geo-fencing technology that prevents a drone from entering restricted areas,[104] among other provisions. He expressed concern that a "patchwork of federal, state, and local restrictions on airspace" creates "significant regulatory confusion."[105] "Piecemeal is not the way to go," declared Governor Brown.[106]

Nevertheless, cities continue to regulate drones, including in Governor Brown's own state. San Diego is currently considering an ordinance that would incorporate the FAA's regulations into its municipal code, deputizing local law enforcement to issue citations for violations.[107] Some states, such as Arizona, Delaware, and Rhode Island enacted legislation in 2016 preventing localities from regulating drones.[108] While local regulations may be well-intended, they are particularly likely to create conflicts with federal law and create a complex and burdensome regulatory environment.

It remains to be seen whether and to what extent courts find that FAA regulation of drones preempts state and local laws. Ultimately, Congress may need to take action so that companies can rely on one set of rules.

> *It remains to be seen whether and to what extent courts find that FAA regulation of drones preempts state and local laws.*

Liability Exposure

While federal regulatory changes are reducing the barriers to drone use, liability risks, including privacy concerns, remain a hurdle to their wider commercial use. Tort litigation involving drones is on the horizon.

> *When an accident occurs, plaintiffs' lawyers are much more likely to file a lawsuit when a drone is operated for commercial use—viewing the owners as a deep pocket—than they are to target a hobbyist.*

FAA INVESTIGATIONS AND FINES

Businesses operating drones must ensure that they comply with FAA regulations. In addition to specific restrictions on operations, the FAA's new drone regulations impose several broad legal duties. For example, operators must maintain drones in condition for safe operation,[109] may not "[o]perate a drone in a careless or reckless manner so as to endanger the life or property of another,"[110] "[a]llow an object to be dropped in a manner that creates an undue hazard to persons or property,"[111] or operate a drone while under the influence of alcohol or drugs.[112] The regulations also require commercial drone operators to report any serious injury to a person or damage to property exceeding $500 within 10 days.[113]

Violations of the small-drone regulations are subject to the existing FAA process for regulatory violations, which may include revocation of a certificate or civil penalties.[114] In January 2017, for example, the FAA announced a settlement agreement with SkyPan International Inc. of Chicago, which specializes in aerial photography of property in urban areas for clients such as developers.[115] The FAA accused the firm of operating drones in congested airspace over Chicago and New York City. SkyPan agreed to pay a $200,000 civil penalty to settle an enforcement action in which the FAA sought a $1.9 million fine.[116]

POTENTIAL TORT LIABILITY

As drones come into routine use, accidents leading to litigation are inevitable. When an accident occurs, plaintiffs' lawyers are much more likely to file a lawsuit when a drone is operated for commercial use—viewing the owners as a deep pocket—than they are to target a hobbyist.

NEGLIGENCE

A 50-pound object—the equivalent of four to five bowling balls—moving as fast as a car, can result in serious injuries or property damage. A drone could crash as a result of a distracted operator or a depleted battery. There is also the potential for a catastrophe if, for example, an inexperienced or uninformed operator flies a drone above the FAA's height limitation or too close to an airport, colliding with a plane. Even before the FAA relaxed drone regulations, the agency logged 1,200 reports of airlines encountering drones in the air.[117] On the other hand, a low-flying drone could distract drivers, contributing to a car accident.

Businesses that operate drones will need to be prepared for negligence claims stemming from such accidents. Case law will set expectations of reasonable care in the drone context. Plaintiffs may attempt to use violations of FAA regulations to establish negligence *per se*.

PRODUCT LIABILITY

Drone manufacturers should also anticipate product liability lawsuits. Much like automakers or aircraft manufacturers, plaintiffs' lawyers are likely to consider suing the company that made the drone by alleging an aspect of the design or the lack of a warning to the operator contributed to an injury. For example, drones come with a wide range of features (and price ranges), some of which can reduce the potential for a collision. Some products include a geo-fencing system that can prevent a drone from flying outside a specified area or height. Manufacturers are developing "sense and avoid" technology that can avoid crashing into trees, buildings, or other obstacles.[118] Eventually, the technology may help drones avoid mid-air collisions with aircraft or other drones.

As these technologies become more widely available, manufacturers whose products do not incorporate state-of-the-art features may face product liability claims alleging there was a safer alternative design. Such lawsuits could threaten to make drones cost prohibitive by eliminating all but the most advanced—and expensive—drones from the market. In addition, warnings that accompany the drone will need to sufficiently alert operators to the risks of harm to themselves and others.[119]

Drone manufacturers may also face lawsuits from third parties alleging that a drone operator would not have injured them or damaged their property if the manufacturer had provided better warnings or instructions on how to safely fly a drone.[120] Such claims may challenge the adequacy of warnings on the packaging, in the owner's manual, and on the drone itself.

When courts consider product liability claims, plaintiffs' lawyers may urge judges to view drone operations as "abnormally dangerous activities."[121] Unlike ordinary product liability claims, which are based on fault, individuals or businesses that conduct abnormally dangerous activities are subject to absolute liability when an injury or property damage occurs related to that activity. This form of super-strict liability applies only when an activity creates a foreseeable and highly-significant risk of physical harm, even when the actor exercises reasonable care.[122]

This doctrine does not apply to common activities, even though dangerous, such as driving cars, because such activities are not deemed abnormal to their surroundings. Courts have applied it to activities such as blasting that throws debris or causes vibrations, damaging neighboring property, or storing hazardous chemicals in a residential area.[123] Before drones come into widespread use, plaintiffs' lawyers may argue for application of this rarely used doctrine. As commercial drone use becomes routine, the likelihood that a court will consider it an abnormally dangerous activity will fall.

> *"Drone use will not only raise negligence and product liability claims, but is likely to spark significant trespass, nuisance, and invasion of privacy litigation."*

TRESPASS

Drone use will not only raise negligence and product liability claims, but is likely to spark significant trespass, nuisance, and invasion of privacy litigation.

Drones typically rely on a mounted camera for navigation, which can capture images or video of people in their backyards and homes. Many drones are specifically used for high-resolution photography. These cameras can intentionally or inadvertently peer into homes and backyards.

Trespass claims based on drone flights reopen the door to the age-old question of where private property ends and the open sky begins. Traditionally, property law recognized *cujus est solum, ejus est usque ad coelum et ad infernos*, which is Latin for "he who owns the soil also owns to the heavens and to the depths."[124] In modern times, the principle may apply in some circumstances (imagine a city building a bridge directly over a house), but not others (such as an airplane flying over that house at 10,000 feet to a nearby airport). Drone flights at a very low level above private property may give rise to a trespass claim.

NUISANCE

Nuisance law requires judicial balancing of the interests involved. Generally, a person is subject to a private nuisance claim if his or her conduct invades another's interest in the private use and enjoyment of land and if the invasion is intentional and unreasonable.[125] In determining whether an invasion is "unreasonable," courts consider whether the gravity of harm to the property owner outweighs the utility of the actor's conduct.[126] Commercial use of drones could give rise to a nuisance claim if, for example, a company's automated drones routinely follow a route directly above a certain individual's property to make deliveries to others, essentially creating a drone expressway above a person's backyard.

The U.S. Supreme Court last addressed a case implicating these areas of law in 1946, when a North Carolina chicken farmer alleged that aircraft landing on a particular runway at an adjacent military airport passed just 63 feet above his barn and 67 feet above his home.[127] The noise and light not only caused him loss of sleep and distress, but led to the death of his chickens, which

> *"The Supreme Court explicitly did not determine the 'precise limits' of airspace within 'the immediate reaches above the land,' which is private property, and airspace that falls within 'the public domain.' Seventy-one years later, it has not answered that question."*

flew into the wall in fright.[128] The Court recognized that the "ancient doctrine that common law ownership of the land extended to the periphery of the universe . . . has no place in the modern world" and that "airspace is a public highway."[129] The Court also indicated that "[t]he airplane is part of the modern environment of life, and the inconveniences which it causes are normally not compensable under the Fifth Amendment."[130] It concluded however, that when flights over private land are "so low and so frequent as to be a direct and immediate interference with the enjoyment and use of the land," they can constitute a taking.[131] The Supreme Court explicitly did not determine the "precise limits" of airspace within "the immediate reaches above the land," which is private property, and airspace that falls within "the public domain."[132] Seventy-one years later, it has not answered that question.

As drones flying over private property become a common part of life, courts will apply a similar analysis in evaluating the viability of trespass and nuisance claims under state common law.

INVASION OF PRIVACY

Drone operators may also face common law invasion of privacy claims. Plaintiffs' lawyers may claim that a drone intrudes upon the seclusion or solitude of their clients. This tort provides that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[133] This determination is likely to be highly fact-specific, imposing the expense of lengthy litigation and a trial.

State statutes will be a factor in the viability of common law trespass, nuisance, and privacy claims. While the FAA's new regulations and some state laws do not address privacy issues,[134] some states have adopted a cause of action for privacy intrusions stemming from drones.[135] Even where a state or local law does not authorize a private right of action, plaintiffs' lawyers may use statutes that address privacy concerns related to drones to support common law claims. The may also contend that courts should find an implied right of action stemming from the law.

> *"Some property owners who come face-to-face with drones have taken the law into their own hands."*

Some property owners who come face-to-face with drones have taken the law into their own hands. Police have arrested people for shooting down drones that fly over their property.[136] A widely reported incident involves William Merideth, a Kentucky man who used his shotgun to take down a drone he believed was spying on his sunbathing teenage daughters.[137] In October 2015, a judge dismissed first-degree endangerment and criminal mischief charges against Mr. Merideth, who calls himself the "drone slayer." The drone owner, his neighbor John Boggs, says he was doing no such thing and disputes how closely the drone came to the house.

Boggs has sued Merideth to recover for his loss of the $1,500 drone and also wants a judge to decide whether his drone was trespassing when it flew over his neighbor's property or was within public airspace.[138] The case, *Boggs v. Merideth*,

is pending in the U.S. District Court for the Western District of Kentucky.[139] As Boggs' lawyer observed, "If every property owner has a right to take a shot at [a drone], that pretty much ends the business model" for companies that would like to use them to deliver packages to customers.[140]

STATUTORY ACTIONS

As noted earlier, businesses using drones must also be cognizant of state and local regulations and private rights of action.

In 2015, the California General Assembly passed legislation that would have armed anyone to sue for trespass if a drone flew less than 350 feet above their property, regardless of whether anyone's privacy was violated. In vetoing that bill, Governor Brown observed that such a law "could expose the occasional hobbyist and the FAA-approved commercial user alike to burdensome litigation and new causes of action."[141]

California then adopted a narrower bill addressing the same issue. It expanded an existing state law that provided a private right of action stemming from a "physical invasion of privacy" to include "airspace above the land of another person without permission."[142] The anti-paparazzi law was initially limited to when "a person knowingly enter[s] upon the land of another without permission to capture any type of visual image, sound recording or other physical impression of a person engaging in a private, personal or familial activity in a manner which is offensive to a reasonable person."[143] Now, a drone operator could face up to three times any damages caused by a violation, as well as a civil fine of $5,000 to $50,000.[144]

While the statute's language would appear to make it unlikely to apply to a company delivering packages or pizzas, businesses may need to carefully obtain permission from consumers to deliver via drone and a waiver of any claims resulting from video of a "private, personal or familial activity" that a drone may capture as it makes a delivery.[145]

Other states have found that there is no need for a privacy law specific to drones. For example, a task force established by the Illinois General Assembly to examine the issue released a report in 2016 finding that state law already provides a means to address voyeurism, harassment, stalking, public nuisance, reckless endangerment, and photographing or recording individuals where there is a reasonable expectation of privacy.[146] The Task Force recommended application of existing laws to conduct involving drones and clarifying, if necessary, certain laws to apply to that context.[147]

INSURANCE COVERAGE

The FAA did not mandate that drone operators obtain insurance coverage in its new small-drone regulations, finding it lacked authority to do so.[148] The agency emphasized, however, that drone operators could be held liable for any injury or damage that results. "Prudent remote pilots should evaluate their existing insurance policies to determine whether they have appropriate coverage for these operations."[149]

Businesses that use drones, or that hire contractors that use drones, will need to verify whether their liability insurance covers injuries or property damage that arise from the drone use. Commercial General Liability (CGL) policies typically cover bodily injury and property damage, but exclude claims arising out of aircraft use (as well as automobile and watercraft use).[150] Insurers are likely to view drones as

falling within this exception. CGL policies also typically protect against negligence, but not intentional torts, which would exclude trespass and intrusion upon seclusion claims from coverage. Even a general aviation insurance policy is unlikely to cover the full scope of claims that could arise from drone use, such as privacy-based lawsuits.

Businesses will either need to add unmanned aircraft liability coverage to their CGL policies or obtain a commercial liability insurance policy that is designed specifically for drone operations. Insurers have begun to offer such policies.[151] Contracts with vendors that use drones should contain FAA compliance obligations, insurance requirements, and an indemnification clause in favor of the contracting party.[152]

The Path Forward

Widespread commercial use of drones relies on continued progress by the FAA to lift restrictions and provide reasonable conditions for safely operating them beyond the line of sight, at night, or over people. This timeline will rely partially on further development of technology, but also on administrative will. The agency's ongoing efforts, which include the close involvement of stakeholders, are promising.

States should resist the urge to adopt drone-specific laws. If they do so, such laws should make clear that they do not create a private right of action. Existing common law principles should be given a chance to work, as they have for other new products and services, when drone-related disputes arise.

The FAA has found that state and local laws that regulate operation of drones are preempted by federal aviation regulation, given the need to keep airspace free of a patchwork of restrictions. If states continue to adopt their own restrictions, then the FAA may need to issue more than a Fact Sheet; it may need to take action.

Private Space Exploration

On February 19, 2017, a rocket lifted off from Kennedy Space Center for the first time since the last space shuttle launch over five years ago.[153] This rocket, a Falcon 9, was sent to resupply the International Space Station, not by the U.S. government, but by the aerospace company SpaceX. As this launch shows, private companies now have a central role in sending cargo, satellites, and people into space. Space tourism is poised to become widely available within the next decade. Will the potential for astronomical liability or regulatory challenges slow innovations from warp speed to impulse power?

Explorers have always faced extraordinary risks. Henry Hudson was likely left adrift in the bay that bears his name after a mutiny of his crew in 1611. In the 1800s, over 20,000 pioneers died along the Oregon Trail while seeking opportunity and a better life in the West. On the way to the South Pole in 1915, Ernest Shackleton's ship, Endurance, became trapped in ice, leaving the crew to attempt to survive on South Georgia Island. Amelia Earhart disappeared over the Pacific Ocean while trying to circumnavigate the globe by plane in 1937. Even today, some of the most experienced climbers have lost their lives while attempting to scale Mt. Everest.

Space exploration is no different. When something goes wrong in space travel, the results are often catastrophic. Lives are lost, as occurred in the 1986 and 2003 Space Shuttle tragedies. Space activities also pose a risk to people and property on the ground. When a rocket explodes, it can result in the loss of high tech payloads and damage to the launch pad, costing hundreds of millions of dollars.[154] As the number of satellites in orbit rises, opportunities for collisions and debris that falls to the Earth's surface also increase.

As space exploration shifts from government-sponsored missions to private industry, will businesses be able to innovate and grow given the liability risks and regulatory challenges?

Today, a patchwork of international treaties, federal laws, and state laws come into play when injury, death, or property damage occurs as a result of space exploration. Only recently have policymakers begun to consider how this framework must evolve to account for the rise of private space exploration.

Unsettled liability questions abound. For instance, what are the requirements for "informed consent," enforceable liability waivers, and insurance coverage when ordinary people participate in spaceflight? How will the FAA regulate commercial spaceports and spaceflights? Does the international obligation to help astronauts in distress extend to space tourists? Can commercial entities engage in space mining without running afoul of a treaty prohibition on acquiring objects in space? Congress and state governments are beginning to provide answers.

The Rise of Commercial Space Exploration

Commercial space activities have significantly increased in recent years.[155] Since 2012, SpaceX and Orbital ATK have resupplied the International Space Station (ISS).[156] The United States, through private companies, is expected to return to manned space travel in 2018.[157] Boeing, for example, is building its CST-100 Starliner, a vehicle capable of taking seven passengers and cargo to low-earth orbit, in a Kennedy Space Center building once used for refurbishing space shuttles.[158] Other companies are developing technology to utilize resources in space.

SPACE TOURISM

Companies such as Virgin Galactic, XCOR Aerospace, Blue Origin, and Stratolaunch System are developing the technology for ordinary people to travel to space at an affordable price.[159] These and other entrepreneurial businesses are building and testing vehicles capable of entering space for a brief period of time, while not entering a sustainable orbit around the earth.[160] Some of these inventions are airplane-like in design, while others use a vertical liftoff and separation with a reusable launch vehicle. Companies have already taken refundable deposits for tickets.[161]

Meanwhile, Space Adventures, a Virginia-based space-tourism company, has arranged for and sent eight clients to the ISS on the Russian Soyuz spacecraft.[162] Most recently, SpaceX announced that it plans to send two paying private individuals around the moon aboard an automated Falcon Heavy rocket in late 2018.[163]

Traditionally, the federal government owned and operated launch facilities, such as the Kennedy Space Center. Now, the FAA's Office of Commercial Space Transportation has licensed ten spaceports in seven states: California, Florida, Texas, Oklahoma, Alaska, Virginia, and New Mexico.[164] Several spaceports are in operation. While some of these facilities are geared for vertical rocket launches, others are designed with space tourism in mind. For example, New Mexico's 18,000-acre Spaceport America hosts SpaceX's Falcon 9R, but has Virgin Galactic as its anchor tenant and is the base of operations for Virgin's aircrafts, WhiteKnightTwo and SpaceShipTwo. While passenger flights have not yet taken place, Spaceport America has held at least 24 vertical launches.[165] There are plans for more spaceports in states such as Colorado, Georgia, and Hawaii.

> *"[T]he FAA's Office of Commercial Space Transportation has licensed ten spaceports in seven states."*

When government entities launch astronauts into space, participants assume the risks. Potential hazards stem not only from a launch or reentry catastrophe, but also from g-forces, high and low pressure, high-decibel noise, radiation, loss of breathable atmosphere, and the effects of weightlessness.

As private companies move into this high-risk area, when an injury or death occurs, participants and their families are likely to file lawsuits against the private companies seeking substantial sums. The ability of spaceflight companies to operate may necessitate fair, legally-enforceable constraints on liability. As this section later discusses, some states have already adopted such laws.

SPACE MINING

One of the reasons space missions are so expensive and limited is the need to transport sufficient water, fuel, and other supplies for the trip. If companies could extract these materials in space, then they could essentially establish gas stations along an interstellar highway.[166] Space mining could be the key to future exploration, enabling people to travel further and live longer in space.

Companies such as Planetary Resources and Deep Space Industries aim to tap asteroids within the next decade. They plan to tap the asteroids for water and then split the water into hydrogen and oxygen to make fuel.[167]

In addition, some materials that are scarce on earth could be acquired elsewhere. For instance, commercial space operations could obtain platinum-group elements that are abundant in asteroids for use in electronics and fuel cells.[168]

International Space Law

Evaluating the legality of space activities and potential liability begins with consideration of international law. The Outer Space Treaty, ratified before the first moon landing, is the primary source of international space law. The treaty requires governments to authorize and supervise the activities of private entities in space.[169] When damage occurs as a result of activity in space, the country that launched or procured the launch of the object is liable to the injured country for damages.[170] The treaty does not distinguish between a launch conducted by the government or a private company, leaving the launching state responsible for the entirety of the damages. In addition, under the treaty, countries have a duty to aid astronauts if there is an accident, distress, or emergency landing on the territory of another state.[171] Among other provisions of the Cold War era agreement is a ban on appropriating objects in space, such as the moon or other celestial bodies.[172]

More specifically, the Convention of International Liability for Damage Caused by Space Objects, ratified in 1972, provides that a launching country is absolutely liable for damage done on the Earth's surface, including loss of life, personal injury, or property damage, as a result of a launch or reentry.[173] If the damage is not to the surface, but in outer space, then the Convention imposes liability based on negligence.[174] While the United States is liable under the treaty, it can seek to recover from a private operator that conducted a launch.

Congress Enters Commercial Space Law

COMMERCIAL SPACE LAUNCH ACT OF 1984

As early as 1984, Congress declared that encouraging commercial space activity is vital for the nation's economic well-being and competitiveness.[175] Regulation, legislators concluded, should be minimal and only to the extent necessary to comply with international obligations, and protect public health and safety, property, national security and foreign policy interests.[176] That law, the Commercial Space Launch Act of 1984, was signed by President Ronald Reagan and provided the FAA with authority to license and monitor commercial launch sites and vehicles.[177]

After the Space Shuttle Challenger accident in 1986, the government transferred responsibility for commercial satellite launches to the private sector.[178] In order to remain competitive internationally and spur growth, Congress amended the Launch Act in 1988 so that private industry and the government would share the inherent risks of space launch.[179] That law requires the company conducting the launch to obtain insurance for claims made by the public up to $500 million, provides government indemnification between $500 million and $1.5 billion (adjusted for inflation), and places liability on the private company for any amount exceeding this level.[180]

COMMERCIAL SPACE LAUNCH AMENDMENTS ACT OF 2004

Congress built on this law in 2004 with the Commercial Space Launch Amendments Act (CSLAA).[181] The CSLAA again calls for private development of launch vehicles designed to carry humans.[182] The law recognizes the "inherently risky" nature of spaceflight and the need for a "clear legal, regulatory, and safety regime" for it.[183] Congress understood that "the regulatory standards governing human spaceflight must evolve as the industry matures so that regulations neither stifle technology development nor expose crew or spaceflight participants to avoidable risks as the public comes to expect greater safety for crew and spaceflight participants from the industry."[184]

In addition to further addressing the FAA's authority to issue licenses and otherwise regulate spaceflights, the CSLAA requires commercial operators to obtain insurance or show financial responsibility for injuries to the U.S. government or third parties.[185] The law requires private operators to inform spaceflight participants of the "risks of launch and reentry, including the safety record of the launch or reentry vehicle type . . . ."[186] Participants must provide written informed consent to engage in spaceflight activities.[187]

FAA regulations implementing the CSLAA specify information that operators must

> *"Regulation, legislators concluded, should be minimal and only to the extent necessary to comply with international obligations, and protect public health and safety, property, national security and foreign policy interests."*

provide to participants in order to obtain informed consent, such as the hazards associated with the flight and the safety record of the launch and reentry vehicles.[188] The regulations also require participants to waive any claims against the federal government, but do not require them to sign waivers with private operators.[189]

The law also introduced a "learning period" that generally precluded the FAA from regulating the safety of commercial spaceflights until 2012, a period that was extended to September 2015.[190] The learning period 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 COMMERCIAL SPACE LAUNCH COMPETITIVENESS ACT OF 2015

With the CSLAA's learning period set to expire, retirement of the Space Shuttle program, and the space tourism industry not advancing as quickly as expected, Congress revisited the law in 2015. As a result, it enacted the Commercial Space Launch Competitiveness Act, also known as the SPACE Act, with broad bipartisan support.[191] This law reduced legal and regulatory barriers for development of space tourism and mining industries.

> *"[T]he SPACE Act. . . reduced legal and regulatory barriers for development of space tourism and mining industries."*

Among its provisions, the law:

- Continues the three-tier approach to liability. A company licensed by the FAA to conduct a launch must purchase insurance covering third-party claims up to $500 million.[193] The federal government indemnifies the company for losses above $500 million up to $3 billion.[193] Any third-party liability claims in excess of that amount are the company's responsibility. The federal government's indemnification of commercial operators covers third-party claims for property damage, and injury or death of the public. It does not indemnify claims brought by those involved in a launch, including spaceflight participants and crew.
- Places exclusive jurisdiction in the federal courts for any death, injury, or property damage resulting from a licensed space launch or reentry.[194] This provision limits forum shopping and is consistent with the federal government's licensing and treaty obligations.
- Promotes development of commercial launch facilities. The law clarifies that states and state launch facilities should take proper measures to cover their potential liability and compensate people for personal or property damage resulting from a launch or reentry.[195]
- Extends the learning period for passenger spaceflight. The law precludes the FAA from issuing regulations unless there is a serious or fatal injury to crew, government astronauts, or spaceflight participants, to 2023.[196]

- Facilitates commercial exploration by clarifying that U.S. citizens, including private companies, can own resources extracted from asteroids or other bodies in space. The law disclaims any intention to exercise sovereignty over any celestial body, consistent with international law.[197]

Predictably, the American Association for Justice (AAJ) decried the 2015 legislation as "terrifying" and mischaracterized it as granting "blanket immunity" to private space travel companies.[198]

> *"Predictably, the American Association for Justice (AAJ) decried the 2015 legislation as 'terrifying' and mischaracterized it as granting 'blanket immunity' to private space travel companies."*

States Provide Incentives for Innovation

Space exploration is an economic driver. According to the FAA, the U.S. commercial space industry accounted for more than $208 billion in economic activity and employed over one million people in 2009.[199] As private companies supply cargo to the ISS, build commercial spaceports, develop new launch vehicles, and prepare to send ordinary people into space, the economic impact here on earth is far greater.

Over the past decade, several states enacted laws designed to attract companies to locate spaceflight operations in their states by limiting their potential liability. Some have also provided tax and regulatory incentives.[200]

> *"Over the past decade, several states enacted laws designed to attract companies to locate spaceflight operations in their states by limiting their potential liability."*

Virginia took the lead when it enacted the Space Liability and Immunity Act in 2007,[201] spurring development of the Mid-Atlantic Regional Spaceport on Wallops Island. Not to be left behind as a space hub, Florida passed its own version of the law, the Informed Consent for Spaceflight Act, in 2008.[202] New Mexico (2010/2013),[203] Texas (2011/2013),[204] California (2012),[205] Colorado (2012),[206] and Oklahoma (2013)[207] soon followed.

These laws recognize that it is impossible to eliminate all of the risks of spaceflight. While the laws vary in language, they concentrate on ensuring that those who board spacecraft are informed of, and accept, these inherent risks. Once a participant reads and signs a written agreement with the legislatively-required information, a spaceflight operator's liability, should an unfortunate event occur as a result of an inherent risk, is limited. Generally, under these laws, an operator is liable if it is grossly negligent, willfully disregards a participant's safety, knew of a dangerous condition, or engages in intentional misconduct that causes an injury.

These spaceflight laws are not novel. They are consistent with express and primary assumption of risk, as recognized in most jurisdictions. They are also similar in purpose and effect to state statutes that protect the ability of people to participate in risky activities, such as skiing or horseback riding. Absent liability constraints and enforceable waivers, these types of activities could become prohibitively expensive for consumers or not offered at all.

States continue to consider new laws. In 2016, the Georgia General Assembly considered a bill viewed as key to developing a commercial spaceport.[208] The Georgia Space Flight Act is similar to the limited liability laws enacted by other states.[209] FAA officials reportedly testified before state lawmakers, telling them that such a law was critical if Georgia was to compete with other states for spaceflight operations.[210] In 2017, as of this writing, the House and Senate each passed a different version of H.B. 1, indicating that it is a top priority in the 2017 session.

Space Insurance Policies

Companies provide insurance for space commerce, but just a few failures in a short period could place the industry severely in the red. In 2015, for example, 3 out of 86 commercial launches failed, resulting in the loss of launch vehicles and payloads.[211]

According to a CNBC report, there are approximately 40 space insurance companies, which individually will provide up to $50 million in coverage per launch.[212] If routine commercial spaceflight takes off, then insured launches will jump from what are now approximately 50 insured launches per year. The potential for multiple, huge losses in a single year will rise.

The Path Forward

The commercial space industry is thriving. It is doing so because Congress, state legislatures, and government agencies have taken a balanced approach to regulatory and liability issues.

Going forward, the spaceflight industry should have the flexibility to develop safety standards that fit new technologies as they become operational. That is the approach Congress took in the 2015 CSLAA, which requires the FAA "to facilitate the development of voluntary industry consensus standards based on recommended best practices. . . ."[213] These standards might address such areas as education and training for spaceflight participants, medical requirements, spaceport features, and launch and reentry safeguards. They should avoid favoring one type of spaceflight vehicle over another. The process of developing consensus standards is already underway.

"The commercial space industry is thriving because Congress, state legislatures, and government agencies have taken a balanced approach to regulatory and liability issues."

In October 2016, ASTM International, which has developed thousands of voluntary consensus standards, approved creation of a technical committee to develop standards for commercial spaceflight.[214]

The FAA should continue to encourage the development of new technology and monitor development of the spaceflight industry. It is inevitable that new spaceflight technology involving human participants will have failures, as it has in the past. When an incident occurs, the FAA should resist the urge to impose heavy-handed regulations that go beyond addressing the specific design feature or practice that resulted in a serious injury or fatality, as Congress intended.

There is room for improving the liability climate for commercial spaceflight. Some have criticized the federal indemnification system as imposing a greater liability risk on commercial space companies than America's competitors, which may lead them to launch elsewhere. In other countries, government indemnification kicks in at a lower dollar level, and only the United States' system includes a third tier that shifts liability for a catastrophic accident back onto the company that conducted the launch.[215]

Others have opined that some of the state statutes limiting liability for inherent risks provide no more protection, and possibly less, than that which spaceflight operators have under existing common law principles in that state.[216] States should continue to adopt carefully drafted laws governing liability for injuries that arise as a result of spaceflight activities, including requirements for enforceable waivers and standards for liability.

The Sharing Economy

Today, people can easily connect with each other to share their cars, homes, and other goods and services. This phenomenon is known as "the sharing economy." The advancement of information technologies and spread of mobile devices have led to a boom in new companies that affect a wide-range of established industries. Ride-sharing and home-sharing services already are valued in the billions of dollars. Will liability risks discourage participation in the sharing economy? Can policymakers strike a regulatory balance that protects consumers without stifling this innovative new sector of the economy?

The sharing economy has experienced rapid growth over the past five years. While still in its infancy, the sharing economy is already generating expected global revenues of $15 billion. These revenues are expected to grow to $335 billion by 2025.[217]

While a few companies have become household names, over 10,000 new companies now participate in the sharing economy.[218] These businesses are disrupting long-established industries and changing the way people buy and sell goods and services. Industries already affected by the sharing economy include hospitality (Airbnb and Couchsurfing), office space (ShareDesk), parking spaces (Parking Panda), transportation (Lyft and Uber), car rentals (Zipcar), outdoor gear (Gearcommons), capital (Kickstarter and LendingClub), medical services (Healthtap), everyday errands (TaskRabbit), and even dog walking (DogVacay). As technology continues to develop, the list of affected industries will continue to expand and evolve.

Over the years, the sharing economy has been referred to as the trust economy, collaborative consumption, on-demand, the gig economy, and the peer-to-peer economy. While there is no universally accepted definition of the sharing economy, it is based on the idea that people do not use their personal property and abilities to their full potential.[219] The sharing economy creates a marketplace that brings people together and allows them to share or exchange underused assets. These assets can be anything from a car, a boat, or a bicycle—to tools, spare time, or an empty room. The sharing economy encompasses

any good or service that can be shared or exchanged for a monetary or nonmonetary benefit.[220]

In a sense, the sharing economy is not new. Throughout history people have bartered and shared unused or underused assets with their families, friends, neighbors and coworkers. However, technology has vastly expanded the pool of potential sellers and consumers. The development of the internet and social media allows people to highlight their underused resources to millions of people worldwide. Improved data storage and analytics make the cost of matching buyers and sellers lower than ever. The development of digital reputations, in the form of user ratings that provide consumers a level of trust, make transactions with complete strangers more comfortable.

Businesses in the sharing economy have developed software platforms that use these advancements in information technology, compiling them into user-friendly, full-featured websites and mobile applications. These new platforms allow service providers and consumers to transact with each other without costly intermediaries. In the process, these platforms collect and distill information about the users to make for transparent interactions. These platforms greatly reduce transaction costs by standardizing the terms of the transaction, facilitating payments, and providing a wealth of information, including the digital reputation of both the supplier and buyer. Without these platforms, suppliers would need to perform nearly all of these tasks on their own, greatly increasing their costs and making such transactions impractical.

The advent and mass spread of smartphones and other mobile devices have further advanced the growth of the sharing economy by allowing people to access web-based sharing services anywhere in the world at any time. An entire transaction, including search, pricing, payment, and evaluation, can be placed onto a single platform and accessed by anyone, whether they are at home or traveling with their smartphone.

Since the barriers to entry are low, the sharing economy enables people to be entrepreneurial and pursue nontraditional forms of income generation. Those looking to make additional money in their free time can provide car rides through a ride-sharing service. A person who frequently travels for work can rent out his or her home for a week at a time. The opportunities for individuals to create their own microbusinesses to generate income are virtually unlimited. In return, the sharing economy benefits consumers by increasing the availability of service providers, lowering costs, and providing altogether new services.

“Since the barriers to entry are low, the sharing economy enables people to be entrepreneurial and pursue nontraditional forms of income generation.”

The Rapid Rise of Ride-Sharing and Home-Sharing

Two of the most rapidly-growing areas of the sharing economy are ride- and home-sharing. These trends show how the sharing economy is creating new value and tapping into markets underserved by long-established industries.

> *"[T]he sharing economy is creating new value and tapping into markets underserved by long-established industries."*

RIDE-SHARING SERVICES

Ride-sharing services provide a platform in the form of a mobile application (app) that facilitates exchanges between private drivers using their personal vehicles and potential passengers looking for a ride. By using an app on their smartphones, passengers are able to request a ride and pay the drivers electronically. The app then provides both the passengers and drivers an opportunity to rate and evaluate each other. The platform sets the fares and collects a percentage of the fare for each completed ride. It is a cash-free transaction.

One such service, Uber, has expanded to provide ride-sharing services in over 500 cities in less than a decade. Over two billion trips have been completed using its app.[222] Uber provides over 100,000 rides per week in most major cities.[223] It had estimated revenue of $1.5 to $2 billion in 2014,[224] and it grew to an estimated $5.5 billion in revenue in 2016.[225] Uber already has an estimated market value of $69 billion, higher than 80 percent of the companies in the S&P 500. [226]

The Uber platform generated an estimated $2.8 billion per year for the U.S. economy in 2014.[227] The company currently employs nearly 7,000 people,[228] and there are over 400,000 drivers that provide rides using the Uber platform in the U.S.[229] In 2015, Uber drivers earned over $3.5 billion.[230] On average, Uber drivers work fewer hours and earn more per-hour than traditional taxi drivers, even after accounting for their expenses.[231] Drivers set their own hours.[232] A third of the drivers are using the platform solely to make extra spending money.[233]

Another large ride-sharing service, Lyft, began in 2012, and is valued at $5.5 billion.[234] Lyft's revenues grew from $200 million in 2015 to $700 million in 2016.[235] Lyft is available in nearly 300 cities.[236] A recent economic study estimated that Lyft added over $170 million to the California economy alone in 2014.[237]

Ride-sharing services expand transportation options. With these additional options, some cities are seeing a drop in drunk-driving.[238] For example, Seattle saw a 10% decrease in DUI arrests following Uber's entrance.[239] Conversely, Austin saw an increase in DUIs after ride-sharing services pulled out of the city.[240] Ride-sharing services also provide inexpensive and reliable service to lower-income neighborhoods in cities where traditional taxis tend to cluster around the wealthiest and densest parts of a city.[241]

HOME-SHARING SERVICES

Airbnb is the largest home-sharing service. It describes itself as "a trusted community marketplace for people to list, discover, and book unique accommodations around the world—online or from a mobile phone or tablet."[242] Airbnb is a matching platform for private homes, connecting hosts with travelers looking for a place to stay, while collecting a booking fee. Its platform aggregates customer reviews, connects users' social media networks to their Airbnb accounts, acts as a secure payment intermediary between host and guest, and provides access to customer support.

In less than 10 years, Airbnb has grown to more than 3 million listings in 191 countries and more than 65,000 cities.[243] In 2015, Airbnb made an estimated $6 billion in bookings.[244] The company is already valued at $30 billion, and its inventory of listings is bigger than the combined listings of Hilton, Marriott, and InterContinental.[245]

While Airbnb and traditional hotels provide a place to stay for travelers, they supply different benefits. For example, families with young children and pets might prefer vacationing in places that provide a yard, playground access, a kitchen, and multiple rooms. Airbnb opens up such amenities to traveling families since many of the hosts are in family neighborhoods. Traditional hotels, on the other hand, have had a hard time providing these amenities since most of the hotel industry's business is generated by corporate travel; hotels must design rooms largely to accommodate business travelers.

In addition, Airbnb has noted that 79% of its travelers wanted to explore a specific neighborhood, and 91% of its travelers wanted to "live like a local."[247] Many of its travelers to New York City stayed in Harlem and Central Brooklyn rather than Times Square, which is heavily populated with hotels. In fact, 74% of Airbnb properties are located outside the main hotel districts, and half of Airbnb guest spending occurs in those neighborhoods, bringing economic support to areas that might not otherwise benefit from tourism.[248] As noted by the CEO of Marriott, Airbnb gives tourists access to neighborhoods that hotels cannot.[249]

Since Airbnb tends to be cheaper than a hotel, consumers who use Airbnb often stay on vacation longer than they would if they stayed elsewhere, and some consumers note that they would not have gone on a vacation without access to Airbnb.[250] An Airbnb-commissioned study found that people staying in San Francisco using Airbnb tended to stay an average of two nights longer and spend on average $260 more in the city than hotel guests.[251] The study also found that 14% of travelers would not have visited San Francisco at all if an Airbnb stay was unavailable, which suggests that the platform is creating a new market rather than just providing an alternative brand.[252] A similar study found that people who used Airbnb stayed on average 2.5 more nights in New York City and spent more money on food and shopping than those who used traditional hotels.[253] The study also indicated that Airbnb services generated $632 million for New York City's economy in 2012.[254]

Airbnb hosts also benefit. In New Orleans, for example, Airbnb hosts makes an average of $70,080 a year hosting.[255] Overall, about half of Airbnb hosts live in low to moderate income households. A little over half (53%) of Airbnb hosts reported that their hosting income allowed them to stay in their home, and 48% of hosts reported that their hosting income allowed them to make ends meet.[258] Other

> *The sharing economy has people engaging in behavior that would have seemed unthinkable just a few years ago.*

hosts reported that they use the money earned from hosting to help support them while going back to school.[259]

Creating Systems of Trust

The sharing economy has people engaging in behavior that would have seemed unthinkable just a few years ago. With ride-sharing, passengers jump into a stranger's car, and with home-sharing, travelers temporarily live in a stranger's house. The converse is equally amazing—homeowners are opening their doors to complete strangers and trusting them to stay in their homes.

The sharing economy has been able to create a level of trust by providing a reputational feedback mechanism that aligns the incentives on both ends of the transaction.[261] Every user has easy access to review and evaluate performance, and all users are interested in a successful transaction in order to maintain their high ratings. This includes the provider of the sharing platform, which also has an interest in a successful transaction and generally provides vetting and screening mechanisms to block questionable or untrustworthy people. This allows the users to evaluate the reputations and results in a reasonably well-functioning, self-regulating market with a strong check on improper behavior.

For example, Uber and Lyft screen their drivers by conducting background checks that review a potential driver's driving history and criminal background.[265] These background check requirements are stricter than the screening requirements that apply to some American taxi drivers.[266] The ride-sharing app shows the driver where the passenger would like to go, and the passenger can see their estimated time of arrival and estimated cost of the ride.

> *This allows the users to evaluate the reputations and results in a reasonably well-functioning, self-regulating market with a strong check on improper behavior.*

Additionally, the passenger and driver have each other's contact information and name so they can text, call, and identify each other. The app allows its users to see the GPS path and monitor the driver-chosen route. When a passenger gives a driver a low rating, he or she will never be matched with that driver again, and drivers that fall below a certain rating level run the risk of being deactivated. Similarly, drivers can decide not to pick up passengers with low ratings.[267]

Similarly, Airbnb also provides an online feedback system to allow guests and hosts to review each other and see the reviews

of other users. Airbnb also records every transaction element for every booking. This tracking includes monitoring the listings, user profiles, reservations, payments, all communications between guest and host, and all follow-up reviews. Airbnb uses this information along with an algorithm it developed to create a "trust score" for each reservation. When a trust score is too low, it is automatically flagged for further investigation by its security team.

For additional security, a host may request an Airbnb representative to visit the host's home to take photos of the space. These photos are then labeled as an "Airbnb.com Verified Photo" on the listing.[269] Airbnb hosts can also require their guests to have a Verified ID Badge, meaning they have verified their identity with Airbnb by submitting a photograph of a government-issued identification.

Airbnb also monitors its system for suspicious activity. For example, it screens for messages that include the words "Western Union," a sign the host is trying to circumvent Airbnb's payment system. A host and guest who repeatedly book rooms with each other could be flagged as they may be trying to build up their reviews or ratings through fake bookings.[270]

Liability Exposure

The sharing economy does involve risk, and accidents and injuries inevitably happen. Some of the worst of these events involving ride-sharing and home-sharing services have gained public and media attention. One such example involved an Uber driver who tragically struck and killed Sofia Liu, a six-year-old girl who was attempting to cross the street with her mother and brother on New Year's Eve.[272] Passengers of ride-sharing services have also reported incidents of assault and battery, sexual assault, and reckless driving.[273] Finally, there have been reports of Airbnb host homes ransacked or burned down, and of stolen property.[274]

In the Liu case, the family brought suit against both the driver and Uber for wrongful death and personal injuries.[275] The family argued that Uber should be held liable for the conduct of the driver under *respondeat superior* and other forms of vicarious liability. Uber denied liability, arguing that it could not be held liable since its drivers are independent contractors and not employees. The parties settled before the court determined whether *respondeat superior* could apply to Uber.

As the Uber case illustrates, businesses in the sharing economy generally classify the individual providers under their platforms as independent contractors, not employees. Companies are ordinarily not liable for the torts committed by their independent contractors, and Uber has successfully relied on this classification to defend itself from liability for torts committed by drivers. For example, in Oklahoma City, passengers brought an action against their driver and Uber, alleging that the driver committed an assault and battery.[276] Uber filed a motion to dismiss, which the court granted, finding Uber was not liable because the driver was an independent contractor and not an employee of Uber.[277] It is unclear, however, as to whether other state courts will consistently adhere to the independent contractor classification of ride-sharing drivers.[278]

Ride-sharing arrangements also raise labor and employment disputes. For example, in Florida, an Uber driver claimed he was entitled to reemployment assistance after Uber revoked his access to the platform based on alleged violations on

Uber's privacy policy.[279] In a February 2017 decision, a state appellate court found that the driver was not an Uber employee because Uber did not maintain the type of control to which a traditional employee is subject.[280] Drivers maintain their own vehicles, choose their own attire, and are not directly evaluated or supervised by Uber, the court found.[281]

> *"[B]usinesses in the sharing economy generally classify the individual providers under their platforms as independent contractors, not employees."*

Drivers have also filed class actions against Uber and Lyft, claiming that the ride-sharing companies misclassify drivers as independent contractors.[282] If considered employees, then Uber drivers claim they are entitled to reimbursement for mileage, overtime pay, tips, and other benefits.[283]

Both companies are attempting to settle these class actions, and as part of both of the proposed settlements, the ride-sharing companies would not have to reclassify their drivers as employees.[284] The companies have not been universally successful, however, in maintaining the independent contractor status of their drivers.[285] For example, the California Labor Commissioner, citing the degree of control Uber exercises over its drivers, ruled that an Uber driver was an employee and could recover from Uber the expenses she incurred while driving.[286] If other courts take a similar approach or the ride-sharing services are unable to retain the independent contractor classification as part of their class action settlements, then ride-sharing services will likely see an increase in employment litigation.

Even if an employer-employee relationship is not established, there are circumstances where a sharing economy company may still be found liable for the tortious acts of an independent contractor. Liability may be in play for independent contractors who have apparent authority, are borrowed servants, or perform non-delegable duties. For example, if a court holds that ride-sharing companies are common carriers, then they may have a nondelegable duty to provide safe transport and could be held liable for the negligence of their drivers. Potentially, liability could also be imposed under a theory of joint enterprise.[287]

Insurance Coverage

Insurance coverage provides an important avenue to compensate people who are injured as a result of participation in the sharing economy. As ride-sharing and home-sharing have developed, insurance coverage has emerged to fit the new business model.

THE EVOLUTION OF INSURANCE COVERAGE FOR RIDE-SHARING DRIVERS

Initially, Uber provided only commercial coverage when its drivers were in the act of transporting passengers, and this coverage was contingent on the driver's personal carrier rejecting the claim. Thus, during the time when the app was on and the driver had not yet selected a ride, as well as the time the driver was en route to pick-up a passenger, the driver was not covered by Uber's policy. In addition, Uber required that drivers maintain a personal auto insurance policy, but these policies typically exclude coverage if the driver is using the vehicle for commercial purposes.

> *As ride-sharing and home-sharing have developed, insurance coverage has emerged to fit the new business model.*

Insurers would assert that the driver should have purchased the more expensive commercial policy, as they were using their vehicle for commercial purposes when the driver was using the app.[288] This exclusion created a potential gap in insurance coverage for accidents that occurred when the driver was using the app but was not actively transporting a passenger.

Following a number of accidents highlighting these insurance gaps, Uber voluntary updated its insurance to provide primary coverage up to $1 million from the moment a driver accepts a trip to its conclusion.[289] Uber also added contingent insurance coverage for the time when the driver has the app open and is waiting for his or her next trip.[290] In addition, Uber worked with a number of other ride-sharing firms, insurance companies, and trade groups to develop model legislation that requires that the ride-sharing services provide liability coverage to protect the drivers, passengers, and third parties who might be injured.[291]

Insurance companies also responded by developing products that are responsive to the unique characteristics of ride-sharing. New plans offered by Allstate, American Family, GEICO, and MetLife Auto & Home take into account the dual professional and personal roles of a ride-sharing driver and attempt to find a middle ground between personal and the much more expensive commercial insurance policies.[292]

AIRBNB DEVELOPS ADDITIONAL INSURANCE PROTECTION

Airbnb has also adapted its insurance coverage. Initially, it provided no insurance.[293] Following an incident where a woman's home was ransacked and essentially destroyed, Airbnb immediately doubled its support staff, offering a 24-hour helpline and instituting a $50,000 insurance policy. Shortly thereafter, Airbnb increased coverage to $1 million. Airbnb has since instituted its Host Protection Insurance Program, covering up to $1 million primary liability for third-party bodily injury or property damage.[294] It expanded the policy in 2015 to cover claims against landlords and homeowners associations from guests who suffer injury during a stay, and claims against hosts filed by landlords for damage caused by guests to a building's property.

Airbnb also offers an online Host Protection Resolution Center. The Resolution Center addresses issues such as claims on security deposits and damage payment requests. The goal of the Resolution Center is to resolve disputes within one week.[295]

Regulators Respond

Critics highlight stories where people have been harmed to suggest the need to regulate home- and ride-sharing as if they are traditional hotels and taxis, respectively. These worst case scenarios, however, are extremely rare. Airbnb successfully completed two million reservations before

its first host sustained severe damage to the home.[296] Overall in 2013, 700 claims were paid to hosts out of approximately 6 million guests, a claim rate of 0.01%.[297] Additionally, Airbnb's response in providing its protection coverage has been described as "freakishly" fast in several high profile cases.[298]

Ride-sharing services have been found to be as safe as, or safer than, traditional taxi rides.[299] One study found taxi drivers are 46% more likely to speed than a ride-sharing driver.[300] Taxi drivers were also found to be 26% more likely than ride-sharing drivers to engage in other unsafe practices such as cellphone use or hard-braking.[301] With this overall safety record, applying regulations governing the taxi and hotel industries to the sharing economy is unwarranted.

While some of the sharing economy remains largely unregulated, the growth and popularity of ride-sharing services have caused local officials to take a variety of approaches to control it.[302] The first approach is an all-out ban, cutting off any potential economic benefits. For example, East Hampton, New York and Panama City Beach, Florida have declared ride-sharing services illegal.[303] At various times, South Carolina, Nevada, and Pennsylvania have taken hard stances to halt ride-sharing operations in their states.[304]

> *"[R]egulations designed for traditional taxi-cabs...are typically ill-suited for ride-sharing services..."*

A second approach involves imposing regulations designed for traditional taxi-cabs. These regulations are typically ill-suited for ride-sharing services and generally result in protecting established taxis rather than improving consumer protection.[305] These regulatory burdens have forced ride-sharing services to completely withdraw from some markets altogether.[306]

Finally, under a third approach, regulators recognize the unique services and benefits offered by new ride-sharing services and draft rules specific to them. For example, California and Colorado adopted rules specific to ride-sharing services.[307] These

> *"The sharing economy is radically changing the way individuals buy and sell goods and services, raising novel regulatory and liability challenges."*

> *Legal and regulatory action should be reserved for situations where there is evidence that a gap in oversight is harming the public, or where there is a need to clarify obligations or inspire consumer confidence.*

rules focus on disclosure requirements, driver background checks, and insurance coverage requirements.[308] The laws also specifically exempt ride-sharing services from the law's definition of "common carrier" and "motor carrier." In addition, the statutes for both states also require that studies be conducted to assess the appropriateness of the minimum liability limits imposed by the new rules.[309] Most states have now followed their example and have enacted similar laws specifically governing ride-sharing services.[310]

The Path Forward

The sharing economy is radically changing the way individuals buy and sell goods and services, raising novel regulatory and liability challenges. It is important that courts and regulators recognize that the sharing economy is a new form of market driven by technology that is rapidly changing.

New regulations should avoid discouraging innovation and competition. Indeed, the sharing economy has grown precisely because the entry barriers are low and existing restrictions have resulted in unmet consumer needs.

Legal and regulatory action should be reserved for situations where there is evidence that a gap in oversight is harming the public, or where there is a need to clarify obligations or inspire consumer confidence. When new requirements are imposed, they should be narrowly tailored so that they are no more restrictive than necessary to serve those goals.

The Internet of Things

A quickly expanding range of everyday items is embedded with technology allowing them to collect and share information. Televisions, home security systems, kitchen appliances, baby monitors, garage door openers, health and fitness monitors, cars, and even pacemakers are among these "smart" devices within the "internet of things" (IoT). This connectivity provides many potential benefits to consumers and businesses. But it also invites hackers, exposing manufacturers to privacy, product liability, and consumer protection claims. There have been few IoT-related lawsuits, but plaintiffs' lawyers say "it's only a matter of time" before the connected world leads to litigation.

An estimated 8.4 billion connected things will be in use in 2017, according to information technology research and advisory company Gartner, Inc. Soon a vast array of man-made physical objects will be able to collect and share data, and some may take action without human intervention.[311] By 2020, some analysts predict that there will be approximately 34 billion[312] to 50 billion[313] connected devices. Only about one third of these devices will be traditional smartphones and tablets, while the remainder will be other "things."[314]

Homeowners may use an app on their phone to set the thermostat and turn the lights on and off. Refrigerators may track and reorder food. Businesses may monitor the flow of products and restock shelves. Cities may embed sensors in roadways to make real-time adjustments to traffic signal timing to fit traffic conditions, while farmers could optimize irrigation schedules by placing sensors in the soil. Even people may be fitted with sensors that allow doctors or caregivers to remotely track a person's health, alert them to a medical emergency, or access data collected by a medical device.[315]

IoT has the potential to contribute trillions of dollars to the economy, allowing consumers and businesses to cut costs and increase efficiency.[316]

Liability Risks

Plaintiffs' lawyers expect that "the next phase of huge product liability litigation" will come from IoT as the number and diversity of connected devices rise.[317]

Manufacturers of connected products face significant liability risks stemming from cyberattacks or the theft of private information. For example, a burglar may access a homeowner's nanny cam to check if anyone is home, and then open the family's garage door through an internet app. A malicious hacker might gain access to a car's electronic system, disabling its brakes or steering, and causing serious injuries or deaths.

Devices that gather images, video, and health information, if compromised, could lead to tort claims for privacy intrusions and both private and government unfair and deceptive trade practices actions.[319] Companies also may face lawsuits claiming that they improperly obtained or used personal data from their connected products.

Liability can also arise from product defects in the software code rather than the physical product. If a remotely controlled thermostat indicates that a house's heating system is operating when it is off, and the pipes burst during the owner's vacation, a lawsuit for property damage is likely to follow. Similarly, if a connected oven or coffee pot overheats, leading to a fire, litigation may focus on whether a coding or communication flaw played a role in the incident.

Government Enforcement

While there is no specific federal law addressing IoT technology, the Federal Trade Commission (FTC) has invoked its general authority to challenge "unfair" practices[320] to take action against companies that allegedly fail to take reasonable measures to detect and prevent unauthorized access to consumer data.[321] The FTC can enjoin the practice at issue, seek restitution for consumers, and, if the business does not comply, seek civil penalties of up to $16,000 for each day of noncompliance.

According to an FTC attorney who focuses on privacy and data security, the agency has brought about 50 IoT-related cases, mostly focused on the "inadequacy of the company's network."[322]

For example, in 2014, the FTC settled an action against TRENDnet, Inc., in which the Commission alleged that a hacker accessed the company's cameras, sold for purposes such as home security and baby monitoring, and posted the feeds for nearly 700 cameras on the internet.[323] The FTC's final order required TRENDnet to establish a comprehensive information security program, obtain third-party assessments of its security programs every two years for 20 years, notify consumers of the breach and the availability of a software update to correct it, and provide free technical support to assist customers to update or uninstall their cameras.[324]

Plaintiffs' lawyers closely watch enforcement actions brought by the FTC and other agencies. Agency action sends a signal that there is an opportunity to

> *"Plaintiffs' lawyers expect that 'the next phase of huge product liability litigation' will come from IoT as the number and diversity of connected devices rise."*

piggyback off the government's investigation by bringing a class action lawsuit alleging a data breach stemmed from a manufacturer's failure to incorporate sufficient security into a connected device.[325]

> *"Plaintiffs' lawyers closely watch enforcement actions brought by the FTC and other agencies."*

The Litigation Begins

Although there are few reports of confirmed hacking into IoT devices, and fewer reports of actual injuries stemming from compromised devices or data, businesses nonetheless face class action lawsuits. These lawsuits, which often rely on a fear of future harm or speculative losses, face significant challenges.

AUTO MANUFACTURERS AND COMPONENT MAKERS: EARLY FIRST TARGETS

Automobiles are increasingly connected to the internet through navigation systems, infotainment systems, integration with mobile devices, and other features. By 2020, it is estimated that one in five cars on the road, or 250 million vehicles, will have some form of wireless network connection.[326]

Ford, General Motors, and Toyota have already been hit with a class action lawsuit alleging that their cars' electric systems are susceptible to hacking.[327] The *Cahen v. Toyota Motor Corp.* lawsuit claimed that it was possible to seize control of a car's throttle, brakes, or steering.[328] The suit relied on the findings of researchers at two universities and a study by the Defense Advanced Research Projects Agency that identified potential vulnerabilities in the vehicles.[329] It alleged that the manufacturers hid the danger from consumers. The word "conceal" appears 223 times in the 342-page complaint.[330] The complaint sought to enjoin the manufacturers from marketing their cars as safe, establish a recall program, and provide free repairs, among other actions.

In November 2015, a federal court dismissed the case. As the trial court properly recognized, courts "regularly deny standing in product liability cases where there has been no actual injury and the injury in fact theory rests only on an unproven risk of future harm."[331] The court viewed the plaintiffs' assertions that their vehicles were worth less as a result of the vulnerability as "conclusory" and "speculative."[332] The ruling is on appeal to the Ninth Circuit.[333]

A separate case against Fiat Chrysler, *Flynn v. FCA US LLC*, is also moving forward. It arose after a July 2015 article in *Wired* in which two cybersecurity experts discussed how they used a vehicle's Uconnect link to the internet to remotely take control of a Jeep Cherokee, altering its climate control and radio, disabling the transmission, and cutting the brakes.[334] Just two weeks later, plaintiffs' lawyers pounced. They filed a class action lawsuit, claiming that the infotainment system in Fiat Chrysler cars suffers from a "hackability defect" that cybercriminals can use to potentially take over vehicles.[335] The lawsuit targets both the automaker and Harman International

"[C]ourts 'regularly deny standing in product liability cases where there has been no actual injury and the injury in fact theory rests only on an unproven risk of future harm.'"

Industries, which manufactures the vehicles' electronic systems. It alleges claims for breach of warranty, fraud, negligence, unjust enrichment, and violation of state consumer protection laws.

The lawsuit remains pending even though the hack was performed by experts after years of research, no owner has actually experienced a hack, and Fiat issued a recall to address the issue within days of the article.[336] In September 2016, a federal district court found that the plaintiffs lacked standing to allege "anxiety or fear" from the possibility of being hacked, finding that a risk of future injury does give rise to a viable claim absent a "substantial" risk that the injury will actually occur.[337] The court, however, allowed claims to proceed alleging that owners overpaid for their cars due to the lost value of the vehicles because of vulnerability to hacking, finding it possible that the recall did not fix all of the issues.[338] The court also allowed a claim for fraudulent concealment to go forward despite what it characterized as "the slight lack of detail" in the complaint alleging how the defendants intentionally withheld information from owners.[339]

MEDICAL DEVICES

After leaving office, former Vice President Dick Cheney revealed that when he needed his implanted defibrillator replaced in 2007, his doctor ordered the wireless feature disabled due to concern that a terrorist could attempt to hack it in an assassination attempt.[340] A decade later, despite the absence of confirmed cases of hackers tampering with connected medical devices, a class action lawsuit was filed.

In August 2016, one day after an investment research firm released a report finding vulnerabilities in cardiac devices that can communicate wirelessly through radiofrequency,[341] lawyers filed a class action lawsuit.[342] The complaint alleges that St. Jude Medical's implantable medical devices that allow for remote monitoring, including pacemakers and defibrillators, have "major security risks," including the possibility that a "bad actor could monitor and modify the implant without necessarily being close to the victim."[343] According to the report relied upon in the lawsuit, a hacker could disable a device through a "crash attack" or a "battery drain attack."[344]

St. Jude responded with a defamation suit against the firm that issued the report, claiming its report spread false and unsubstantiated information in an attempt to profit by driving down its stock price.[345] The plaintiff voluntarily dismissed the action against St. Jude without prejudice in December 2016.[346] The defamation lawsuit is pending.[347]

CHILDREN'S TOYS

Companies that make and sell products to children are often viewed as an attractive

target by plaintiffs' lawyers. That is also the case for IoT liability. As a plaintiffs' lawyer who has brought IoT cases candidly acknowledged, his firm started by looking at products aimed at children and seniors.[348] Mattel and VTech have faced such claims.

> *"As a plaintiffs' lawyer who has brought IoT cases candidly acknowledged, his firm started by looking at products aimed at children and seniors."*

In the Mattel suit, filed in Los Angeles Superior Court in December 2015, two mothers claimed Hello Barbie records children's voices without parental consent.[349] The doll is designed to engage in conversation with children six years old and older. When a child presses the belt buckle the doll records the conversation and sends it via WiFi to a cloud database.[350] A parent activates this feature by downloading a smartphone app that allows the parent to play, share, or delete the recordings. The class action alleged that while the toy's owner may consent to the toy recording his or her child, when the toy records conversations of playmates and other children, the company violates the Children's Online Privacy Protection Act. The complaint also included claims for negligence, unjust enrichment, and invasion of privacy.

After the case was removed to federal court, it was voluntarily dismissed with prejudice by the parties.[351] Meanwhile, privacy groups have expressed broader concerns with other internet-connected "spy toys," alleging in a December 2016 complaint with the FTC that they "subject young children to ongoing surveillance and are deployed in homes across the United States without any meaningful data protection standards" and "pose an imminent and immediate threat to the safety and security of children in the United States."[352]

VTech has faced several class actions alleging privacy violations after an overseas hacker breached its database in November 2015, which allegedly included photos, chat logs, and voice messages associated with its children's learning toys.[353] The breach affected the accounts of over two million parents and nearly three million children in the United States, and many more abroad.[354] VTech filed a motion to dismiss in April 2016, arguing that despite sensational media coverage, the plaintiffs' claim amounted to no more than a fear of future injury.[355] According to VTech, this fear is not an actual or imminent harm because the compromised information "made it no farther than an arrested hacker who sent samples to one media outlet and one consulting analyst."[356]

Because the parties indicated in early 2017 that they are engaged in settlement discussions,[357] the court has not ruled on the motion to dismiss.

How Will IoT Affect Tort Law?

Litigation resulting from IoT products may place renewed focus on several legal doctrines.

THE NEED FOR STANDING

As the litigation against automakers shows, before a court will consider their claims, plaintiffs must establish standing. As noted above, litigation stemming from hacking of cars or expressing concern

about the security of medical devices has not involved actual injuries, but primarily makes claims that the products' security vulnerability creates a risk of harm. IoT-related lawsuits may also argue that vulnerability could lower the value of a product, asserting that a consumer paid too much to purchase the product or that the resale value has diminished.

Such speculative, no-injury claims are likely to be dismissed. Courts will look to the Supreme Court's 2013 ruling in *Clapper v. Amnesty International*, in which it held that a plaintiff must allege more than speculative fears to establish standing under constitutional standards.[358] In that case, several groups claimed that the threat of being monitored by the U.S. government as a result of the Foreign Intelligence Surveillance Act violated their constitutional rights, but they only alleged an abstract subjective fear of being monitored. While *Clapper* does not preclude all lawsuits based on a threat of future harm, claims must show a "certainly impeding" harm, not just a "possibility" of future injury.[359] This standard may not require literal "certainty," but it at least requires a "substantial risk" that the harm will occur.[360]

Courts will also consider the U.S. Supreme Court's 2016 decision in *Spokeo, Inc. v. Robins*, where the Court emphasized that the alleged injury "must affect the plaintiff in a personal and individual way," and "must actually exist."[361] A "conjectural or hypothetical" claim of injury does not create standing.[362]

Absent evidence of actual hacking (not merely a researcher showing that someone can theoretically hack a product) or evidence showing that the resale value of the product actually declined or otherwise led to owner losses as a result of the vulnerability, such claims have little chance of success.

CRIMINAL CONDUCT OF THIRD PARTIES

In lawsuits stemming from the hacking of a product, tort law principles addressing a party's liability for the criminal acts of third parties may come into play. Such principles often arise in the context of premises liability and nuisance claims.

Traditionally, there is generally no duty to warn or protect another from the intentional torts or criminal acts of third parties.[363] The law evolved to recognize a limited duty when there is a "special relationship" between the plaintiff and defendant, such as common carrier-passenger, innkeeper-guest, or business-invitee.[364] If such a relationship exists, then courts consider whether the criminal act was reasonably foreseeable to the defendant, based on such factors as where the crime occurred, the frequency of criminal incidents, the similarity of past crimes, and any prior knowledge of threats. When these two factors are fulfilled—a special relationship and a foreseeable harm—then a business has a duty to take

> *"While* Clapper *does not preclude all lawsuits based on a threat of future harm, claims must show a 'certainly impeding' harm, not just a 'possibility' of future injury."*

> *[T]ort law would not impose liability on an automobile manufacturer where a third party intentionally cut the brake line. Nor would a homebuilder face liability after a skilled burglar broke through the roof of a home.*

steps to prevent the harm. Even then, the plaintiff will not be successful if the injury would have occurred even if the defendant had taken the steps sought.[365]

Applying these principles, tort law would not impose liability on an automobile manufacturer where a third party intentionally cut the brake line. Nor would a homebuilder face liability after a skilled burglar broke through the roof of a home. IoT-related torts have similarities to these scenarios, but are more complex, alleging that the design of a product included a vulnerability that was exploited. In addition, since the identity of a hacker may not be known or that person may be located beyond the reach of the courts, consumers are likely to target the manufacturer in a lawsuit seeking recovery.

A POST-SALE DUTY TO WARN AND RECALL?

As software glitches emerge, vulnerabilities are identified, and hackers become more sophisticated, manufacturers of IoT products may have obligations to monitor their products, warn consumers of risks, and provide software patches throughout the life of the product.

Traditionally, tort law did not place an ongoing duty on manufacturers to warn consumers if they learn of a potential product hazard after selling a product.[366] Distinguished law professors have recognized that a "post-sale duty to warn" is troubling to manufacturers because, if not tightly confined, it imposes a timeless "monster duty."[367]

> *[A] 'post-sale duty to warn' is troubling to manufacturers because, if not tightly confined, it imposes a timeless 'monster duty.'*

After vigorous debate, however, the American Law Institute included a post-sale duty to warn in the Restatement (Third) of Torts: Products Liability, finding that, despite a split in authority, a sufficient number of jurisdictions had adopted the theory in some form.[368] It restricted this duty, however, to situations in which: (1) a seller knows or should know a product

imposes a substantial risk of harm; (2) a seller can identify those to whom a warning might be provided and reasonably assume they are unaware of the risk of harm; (3) a seller can effectively communicate a warning so that it is acted upon; and (4) the risk of harm is sufficiently great to justify the burden of providing a warning.[369]

The Restatement (Third) also recognizes a duty to recall a product in only two circumstances: (1) when required by government regulations; or (2) when voluntarily undertaken, if done negligently.[370] Thus, recall obligations are primarily based on statutory law. Depending on the type of product at issue, manufacturers have post-sale reporting and recall obligations to the Consumer Product Safety Commission, FDA, NHTSA, or FTC. Failure to report such hazards may result in significant civil penalties.

It is uncertain where IoT-related liability will fall when a product warranty ends, or a product's manufacturer no longer makes a product or is no longer in business.

As more devices come online, additional courts may adopt, and some may expand, post-sale duties to warn and recall products. Reporting and recall obligations in a product-connected world will, in any event, become better understood over time.

Insurance Coverage

Given the substantial but not-fully-known liability risks in providing connected devices, manufacturers will need to evaluate whether they have adequate insurance coverage. Because of the wide range of potential losses, IoT will implicate various types of policies.

In terms of first-party property policies, which protect the policyholder against losses suffered by the policyholder itself, coverage should contemplate not only physical property damage in case of destruction (e.g., by fire or water damage), but also the value of the data residing in the object that was damaged. With respect to third-party policies, manufacturers that are named in product liability lawsuits stemming from a connected feature of a product will face challenging coverage questions unless the policy is specifically tailored to the unique qualities of the IoT device manufactured, sold, or used by the policyholder.

IoT stakeholders cannot assume that their Commercial General Liability (CGL) insurance policies will be sufficient to protect them against IoT-related claims. For example, it is uncertain whether a standard CGL policy exclusion that applies when work has not yet been completed or abandoned would void coverage when a product continues to communicate using an algorithm that is accessed and refined by the manufacturer. Many traditional liability policies also contain broad electronic data exclusions to which IoT devices may succumb.

As a result of the increase in connected devices, the cyber insurance market has had a surge of interest. Companies are indemnifying against first- and third-party losses that might result from a data breach of personally identifiable information, company network disruption, cyber extortion, and media liability.[371] Only a few insurers have developed the nuanced and sophisticated policies required by IoT, and even those policies are likely to be subject to various interpretations by insurers, policyholders, and courts.

Coverage disputes are a time-consuming and costly endeavor, making it important for manufacturers and insurers to determine whether their policies extend to the various risks posed by IoT.

Congress Wades In

No specific federal law addresses IoT, but over the past two years, Congress considered bills both pushing for the advancement of this technology and responding to privacy concerns.

In March 2015, the U.S. Senate unanimously passed a resolution recognizing the promise of IoT for increasing economic opportunity, empowering consumers, and cutting costs. The resolution called for a national strategy to "prioritize accelerating the development and deployment of the Internet of Things in a way that recognizes its benefits, allows for future innovation, and responsibly protects against misuse."[372]

The following year, the same bipartisan group of senators that sponsored this resolution introduced the "Developing Innovations and Growing the Internet of Things Act," known as the DIGIT Act.[373] The bill would have created a working group of federal agencies, housed within the Department of Commerce, to provide recommendations to Congress on how to encourage the growth of IoT. The working group would be advised by a steering committee of stakeholders from outside the federal government, including small business and rural stakeholders.[374] The Senate Committee on Commerce, Science, and Transportation favorably reported the bill in September 2016,[375] and again in January 2017.[376] The Senate bill and House companion bill remain pending.[377]

Federal legislation has also been proposed to address concern that cars are collecting data that may not be sufficiently secured. The Senate iteration—the Spy Car Act—would require the National Highway Traffic Safety Administration (NHTSA) to conduct rulemaking to issue cybersecurity regulations that require manufacturers to secure driving data, such as a vehicle's location or speed, from unauthorized access. The legislation would also have instructed the FTC to promulgate a rule requiring manufacturers to provide information to vehicle owners and lessees about how vehicles collect data, give consumers an option to terminate data collection and retention, and prohibit manufacturers from using collected information for advertising or marketing purposes without consent.[378] The House version would instruct NHTSA to conduct a study, rather than promulgate a rule, to determine and recommend standards for the regulation of the cybersecurity of motor vehicles.[379] Neither approach has advanced.

> *"At least five federal agencies have recently undertaken efforts to address IoT-related issues."*

A Flurry of Federal Agency Guidance on IoT Safeguards

At least five federal agencies have recently undertaken efforts to address IoT-related issues. While their guidelines are nonbinding, they are likely to influence agency enforcement efforts under existing regulations. In addition, courts may look to these standards, as well as industry practices, to determine a standard of care in private lawsuits.[380]

FTC (JANUARY 2015)

The FTC released a detailed staff report, "Internet of Things: Privacy & Security in a Connected World," which addresses how companies can build security into connected devices, minimize data collection, and

provide information to consumers about how their data will be used.[381] The FTC finds that enacting IoT-specific legislation would be premature and could impede innovation, preferring instead that particular industries develop self-regulatory programs on privacy and security practices.[382] The FTC concurrently released a separate document, "Careful Connections: Building Security in the Internet of Things," which provides brief, easy-to-read tips for businesses to build security into IoT devices.[383] These materials are particularly important given the wide range of products that fall under the FTC's jurisdiction and its ability to bring enforcement actions.

NHTSA (OCTOBER 2016)

NHTSA released best practices for automotive cybersecurity.[384] While there are no motor vehicle safety standards specific to cybersecurity, the NHTSA report reminds manufacturers that they have a general legal obligation to ensure that vehicles are free of unreasonable risks to safety, which includes risks resulting from cybersecurity vulnerabilities.[385]

DHS (NOVEMBER 2016)

The Department of Homeland Security (DHS) published a set of "strategic principles" for securing the IoT.[386] The report concludes by encouraging dialogue on "how tort liability, cyber insurance, legislation, regulation, voluntary certification management, standards-setting initiatives, voluntary industry-level initiatives, and other mechanisms could improve security while still encouraging economic activity and innovation."[387]

FDA (DECEMBER 2016)

The Food and Drug Administration (FDA) finalized guidance identifying key areas that medical device manufacturers should focus on to maintain an effective post-market cybersecurity program.[388] The FDA emphasizes that medical device cybersecurity is a "shared responsibility" among healthcare facilities, patients, and providers as well as device manufacturers.[389] However, if a patient injury or death occurs, potentially as a result of a cybersecurity breach, observers recognize that "manufacturers are likely to be the front line of any litigation."[390]

> *"The Department pledges to develop policies that ensure that the IoT environment is inclusive and accessible, stable and secure, and built on industry-driven consensus-based standards."*

DEPARTMENT OF COMMERCE (JANUARY 2017)

The Department of Commerce released a draft "Green Paper."[391] The Department observes that IoT has the potential to benefit public safety, healthcare, governance, and the environment.[392] While the Department recognizes that "specific policies may need to be developed" for certain areas of IoT technology, it finds that, overall, "the challenges and opportunities presented by IoT require a reaffirmation rather than a reevaluation of this well-established U.S. Government policy approach to emerging technologies."[393] The Department pledges to develop policies that ensure that the IoT environment is inclusive and accessible, stable and secure, and built on industry-driven consensus-based standards.[394] It vows to encourage

IoT growth and innovation by reducing barriers and encouraging coordination among all stakeholders.[395]

The Path Forward

Eventually, most, if not all, devices will be connected. The phrase, the "Internet of Things," will quickly become obsolete as an internet connection becomes as common as a product plugged into an electrical outlet.

While IoT poses new and unique risks, particularly with regard to data security, existing legal principles should govern any resulting litigation. Product liability, invasion of privacy, consumer protection, and other traditional causes of action will fit IoT devices.

Constitutional principles requiring standing should preclude speculative lawsuits that allege no more than the presence of a security vulnerability in the product that theoretically could lead to a breach. Actual harm, not a hypothetical harm or fear of a future injury, is required.

When breaches occur, courts are likely to look to industry best practices and agency guidance to evaluate whether a manufacturer incorporated adequate security into a connected device. Product liability claims will turn on whether there was a reasonable and feasible alternative design that would have avoided the vulnerability.

There are, however, open questions and the potential for expanded liability. Plaintiffs' lawyers are likely to push courts to evaluate design defects not at the time of sale, as traditionally required, but, given the ability to update connected devices, on an ongoing basis. For the same reason, they may urge courts to adopt a broad post-sale duty to warn and common law recall obligations. In the context of connected devices, courts may shift from viewing the criminal acts of third parties as intervening causes to foreseeable risks for which a manufacturer has a duty of care to protect against.

> *"The phrase, the 'Internet of Things,' will quickly become obsolete as an internet connection becomes as common as a product plugged into an electrical outlet."*

In sum, while consumers are attracted to the benefits of connected devices, fulfilling this demand comes with significant liability risks for product manufacturers. They should enter this new connected world cautiously, adopt state-of-the-art security measures, and obtain insurance coverage that fully covers their liability exposure.

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

The challenge of 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 autonomous vehicles to connected devices—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 has distinct challenges, lessons can be drawn that apply across the board as courts, legislators, and regulators grapple with these changes.

Principles of Liability

TRADITIONAL PRINCIPLES OF LIABILITY SUFFICIENTLY ADDRESS MOST CLAIMS THAT ARISE AS A RESULT OF EMERGING TECHNOLOGIES

Legislatures should not enact new private rights of action specific to emerging technologies. For example, several states have unnecessarily created new rights for property owners to sue when drones fly on or near their property, where trespass, nuisance, and privacy claims would already provide a remedy. If state and local governments enact laws regulating drone operations, they should make clear that the enforcement mechanism and penalties in the regulation are exclusive and that courts should not use the standards to create "implied" rights of action or as predicates for tort claims.

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

For example, courts should not impose strict liability on auto manufacturers for every accident involving an autonomous vehicle, effectively turning every car accident into a product liability claim. Nor

should courts abandon the long-recognized distinction between employees and independent contractors to impose liability on companies that provide platforms that facilitate the sharing economy. Traditional tort principles that significantly constrain the liability of manufacturers for the criminal acts of third parties or limit the duty to warn after a product is sold should not be abandoned as more connected products enter the market.

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

As courts have recognized, a potential vulnerability in a connected product, absent actual harm to a consumer, does not give rise to a viable claim.

WHERE LIABILITY EXPOSURE POSES A THREAT TO AN EMERGING TECHNOLOGY, LEGISLATORS SHOULD ADOPT REASONABLE CONSTRAINTS ON LIABILITY

For example, Congress and several states have placed bounds on liability involving private space travel, recognizing the potential for extraordinary losses and the inherent risks of the activity. As a result, American rockets are resupplying the International Space Station and are expected to soon carry astronauts to the ISS, the moon, and Mars; spaceports are opening; and development of vehicles for space tourism and mining are rapidly advancing.

COURTS SHOULD CLOSELY CONSIDER WHETHER STATE LAWS, INCLUDING TORT CLAIMS, INVOLVING AN EMERGING TECHNOLOGY ARE PREEMPTED WHEN THAT PRODUCT OR SERVICE IS REGULATED BY FEDERAL LAW

Overlapping and potentially conflicting federal, state, and local regulation of drone operation, for example, is likely to pose a serious impediment to the ability of businesses to use the new technology without an unreasonable risk of inadvertently violating the law or subjecting itself to liability. FAA regulations should provide a uniform source of operator rights, obligations, and restrictions. Federal agencies can help by clearly asserting their intent to preempt state law in regulations, agency guidance, and amicus briefs filed with courts.

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

The new business models in the sharing economy emerged to fulfill consumer needs that were unmet at least in part due to regulations and costs imposed on established industries. Applying burdensome or ill-fitting regulations reduces consumer choice and hurts entrepreneurship.

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

For example, Congress has adopted a "learning period" that prohibits the FAA from regulating the safety of commercial spaceflights until 2023. 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.

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

As California Governor Jerry Brown recognized in vetoing several bills that would have imposed restrictions on drone operations, a "patchwork of federal, state, and local restrictions" creates "significant regulatory confusion."[396] "It's more prudent to explore a more comprehensive approach that takes into account federal regulations. . . Piecemeal is not the way to go."[397]

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

This has led companies like Airbnb to provide hosts with insurance and guests with a dispute resolution center. Ride-sharing services voluntarily conduct background checks on drivers and provide a feedback system that encourages high-quality service. A wide range of stakeholders are participating in developing regulations to expand safe drone use. Auto manufacturers have stated that they will assume liability for accidents involving their autonomous vehicles, particularly during the start-up phase. Businesses are developing voluntary industry consensus standards for various aspects of spaceflight, such as education and training for participants, medical requirements, spaceport features, and launch and reentry safeguards. Before acting, regulators should carefully examine whether imposing new legal requirements is warranted in light of existing safeguards.

WHEN REGULATION IS WARRANTED, IT SHOULD BE DEVELOPED THROUGH CLOSE COLLABORATION WITH STAKEHOLDERS THAT FULLY UNDERSTAND THE EMERGING TECHNOLOGY

Such a process can result in sound policies, facilitate growth of emerging technologies, and bolster consumer confidence.

GOVERNMENT AGENCIES SHOULD COORDINATE THEIR RESEARCH AND REGULATION OF EMERGING TECHNOLOGIES

For instance, in the span of a few months, five federal agencies released guidance to manufacturers on addressing IoT-related security concerns, even as Congress considered legislation to establish a federal working group to coordinate such efforts.

Endnotes

† The authors appreciate the constructive suggestions on this manuscript provided by Victor E. Schwartz, our law partner and coauthor of the casebook, Prosser, Wade & Schwartz, Torts: Cases and Materials (Foundation Press 13th ed. 2015).

1 Michele Bertoncello & Dominik Wee, Ten Ways Autonomous Driving Could Redefine the Automotive World, McKinsey & Company Automotive & Assembly, June 2015.

2 *See* Insurance Institute for Highway Safety Loss Data Institute, Fatality Facts: Yearly Snapshot (Nov. 2016) (reporting 35,092 motor vehicle crash fatalities in 2015).

3 Alan D. Kaplan & Robert Sanzillo, Driverless Cars, Prod. Liab. L. & Strategy, Aug. 2016.

4 Eno Center for Transportation, Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations 8 (Oct. 2013).

5 *Id.*

6 *See* KPMG, Automobile Insurance in the Era of Autonomous Vehicles 5 (June 2015).

7 Eric Kroh, Fault Lines: How Driverless Cars Could Open Up New Roads for Product Liability Lawyers, Law360, Mar. 18, 2016.

8 *Id.*

9 Nat'l Highway Transp. Safety Admin., Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety 5 (Sept. 2016).

10 *Id.* at 45.

11 *Id.* at 46.

12 *See* SAE Int'l, Automated Driving: Levels of Driving Automation are Defined in New SAE International Standard J3016 (2014).

13 *See* KMPG, *supra*, at 5.

14 *See id.* at 3.

15 Nat'l Highway Traffic Safety Admin., Vehicle to Vehicle Communications: Readiness of V2V Technology for Application 17 (Aug. 2014).

16 Danielle Muoio, 19 Companies Racing to Put Self-Driving Cars on the Road by 2021, Business Insider, Oct. 17, 2016.

17 *See* Rachel Abrams & Annalyn Kurtz, Joshua Brown, Who Died in Self-Driving Accident, Tested Limits of His Tesla, N.Y. Times, July 1, 2016.

18 *See* Tesla, A Tragic Loss (blog post), June 30, 2016.

19 *See* Nat'l Highway Traffic Safety Admin., ODI Resume, Investigation PE 16-007 (Closed Jan. 19, 2017).

20 *Id.*; s*ee also* Danielle Muoio & Reuters, The Government Just Closed its Investigation into the First Autopilot Fatality, Business Insider, Jan. 19, 2017.

21 *See* Tim Higgins, Google's Self-Driving Car Program Odometer Reaches 2 Million Miles, Wall St. J., Oct. 5, 2016.

22 Joseph Serna, Video Shows Google Self-Driving Car Hit a Bus in Silicon Valley, L.A. Times, Mar. 9, 2016.

23 Ben Seal, What Happens if a Self-Driving Uber Is in a Crash?, Law.com, Sept. 16, 2016.

24 *See* Michael Isaac, Uber Expands Self-Driving Car Service to San Francisco. D.M.V. Says It's Illegal, N.Y. Times, Dec. 14, 2016.

25 *See* Christopher Mele, In a Retreat, Uber Ends Its Self-Driving Car Experiment in San Francisco, N.Y. Times, Dec. 21, 2016.

26 *See* Trisha Thadani, Uber Sending Self-driving Cars to Arizona, S.F. Chron., Dec. 22, 2016. Uber is now reportedly planning on applying for the California permit. *See* Marisa Kendall,

Uber to Apply for California Permit to Test Self-driving Cars, Mercury News, Mar. 2, 2017.

27 Office of the Governor, Press Release, Governor Ducey Tells Uber 'CA May Not Want You, But AZ Does', Dec. 22, 2016.

28 Alexandria Sage, Ford to Invest $1 Billion in Autonomous Vehicle Tech Firm Argo AI, Reuters, Feb. 10, 2017.

29 Adam Thierer, When the Trial Lawyers Come for the Robot Cars, Slate.com, June 10, 2016; *see also* Douglas Newcomb, Will Lawsuits Kill the Autonomous Car?, MSN Autos, Apr. 15, 2013; Dan Strumpf, Liability Issues Create Potholes on the Road to Driverless Cars, Jan. 27, 2013.

30 *Id.*

31 Chris Nichols, Liability Could Be Roadblock for Driverless Cars, San Diego Trib., Oct. 30, 2013.

32 John Villasenor, Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation 13-14 (Center for Technology Innovation at Brookings, Apr. 2014).

33 *See* Hope Reese, When Your Driverless Car Crashes, Who Will Be Responsible? The Answer Remains Unclear, Tech Republic, Sept. 7, 2016.

34 Keith Naughton, What Happens if Two Driverless Cars Crash? Lawyers Drool, Bloomberg News, Dec. 22, 1015.

35 Cal. Vehicle Code § 38750; Nev. Rev. Stat. §482A.030.

36 Brian Fung, The Big Question About Driverless Cars No One Seems Able to Answer, Wash. Post, Feb. 17, 2016 (emphasis in original).

37 Kroh, *supra*.

38 *Larsen v. Gen. Motors Corp.*, 391 F.2d 495, 502 (8th Cir. 1968).

39 Ryan Abbott, Draft Working Paper: The Reasonable Computer: Disrupting the Paradigm of Tort Liability, at 22 (last revised Feb. 4, 2017).

40 *Id.*

41 Kroh, *supra*.

42 *Id.*

43 Am. Assoc. for Justice, Driven to Safety: Robot Cars and the Future of Liability (Feb. 2017).

44 *Id.* at 4-5.

45 *Id.* at 27.

46 *Id.* at 27-28.

47 James M. Anderson et al., Autonomous Vehicle Technology: A Guide for Policymakers (RAND Corp. 2016).

48 *See* Health Resources & Services Admin., About the National Vaccine Injury Compensation Program, *at* https://www.hrsa.gov/vaccinecompensation/about/index.html (last visited Feb. 27, 2017).

49 Nidhi Kalra, James M. Anderson & Martin Wachs, Liability and Regulation of Autonomous Vehicle Technologies (RAND Corp., Apr. 2009).

50 Corine Iozzio, Who's Responsible When a Self-Driving Car Crashes, Scientific American, May 1, 2016.

51 Daniello Muoio, Elon Musk: Telsa Not Liable for Driverless Car Crashes Unless It's Design Related, Business Insider, Jan. 4, 2017.

52 *Id.*

53 *See* ODI Resume, Investigation PE 16-007, *supra*, at 10-11; *see also* Tom Randall, Tesla's Autopilot Vindicated With 40% Drop in Crashes, Bloomberg Technology, Jan. 19, 2017.

54 *See* Fed. Aviation Admin., Final Rule, Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42064 (June 28, 2016) (effective Aug. 29, 2016) (to be codified as 14 C.F.R. pt. 107).

55 *See* Alina Selyukh, FAA Expects 600,000 Commercial Drones in the Air Within a Year, NPR, Aug. 29, 2016.

56 FAA Aerospace Forecast: Fiscal Years 2016-2036, at 31 (2016).

57 *See* FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11, 75-76, § 333.

58 *See* Fed. Aviation Admin., Unmanned Aircraft Systems, Section 333, *at* https://www.faa.gov/uas/beyond_the_basics/section_333/ (last visited Feb. 13, 2016) (indicating 5,551 Section 333 petitions approved as of Sept. 28, 2016).

59 *See* Timothy Q. Purdon & Seth A. Nielsen, FAA Regs for Small Drones – A Stop in the Right Direction, Law360, July 12, 2016.

60 *See* Mike Orcutt, Now You Can Finally Use Your Drone to Make Money, Tech. Rev., Aug. 26, 2016; *see also* Aldo Fucentese & Michael Mills, 10 Steps to Mitigate Drone Risks on Construction Sites, Property Casualty 360, Nov. 8, 2016.

61 *See id.*

62 *See* Clay Dillow, Why 2015 is the Year Agriculture Drones Take Off, Fortune, May 18, 2015.

63 *See* Orcutt, *supra*.

64 FAA Allows Commercial Use of Small Drones, PBS News Hour, June 21, 2016; see also Amazon Prime Air, *at* www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011 (last visited Feb. 16, 2017) (announcing testing of service that uses autonomous drones to deliver packages of up to five pounds in 30 minutes or less).

65 *See* Pie in the Sky: Russian Chain Delivers Pizza By Drone, N.Y. Daily News, June 25, 2014; Your Drone Arrived! Russian Pizzeria Launches Unmanned Delivery, Russia Today, June 23, 2014.

66 *See* Jeremy Bradley, It's One Delicious Drone – the Burrito Bomber, CNN, June 21, 2013.

67 *See generally* FAA Fact Sheet – Small Unmanned Aircraft Regulations (Part 107), June 21, 2016.

68 *See* FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11, 72, §331(6); 81 Fed. Reg. at 42,209 (to be codified at 14 C.F.R. § 107.3).

69 *See* 81 Fed. Reg. at 42,210-11 (to be codified at 14 C.F.R. §§ 107.29, 107.31, 107.39, 107.51).

70 *See* 81 Fed. Reg. at 42,213 (to be codified at 14 C.F.R. §§ 107.200, 107205).

71 Fed. Aviation Admin., Advisory Circular No. 107-2, at 5.19.2 (June 21, 2016).

72 See Fed. Aviation Admin., Request a Waiver/Airspace Authorization Small Unmanned Aircraft System (sUAS), *at* https://www.faa.gov/uas/request_waiver/ (last visited Feb. 13, 2017).

73 *See* Fed. Aviation Admin.,Part 107 Waivers Granted, *at* https://www.faa.gov/uas/request_waiver/waivers_granted/ (last visited Feb. 13, 2017).

74 *See* Orcutt, *supra*.

75 FAA Aerospace Forecast: Fiscal Years 2016-2036, at 31-32 (2016).

76 *Id.*

77 *Id.*

78 *See* Fed. Aviation Admin., Press Release, FAA Unveils Effort to Expand the Safe Integration of Unmanned Aircraft, Feb. 24, 2016 (announcing establishment of aviation rulemaking committee including industry stakeholders with goal of providing recommendations on drone operation above people by Apr. 1, 2016).

79 *See* Micro Unmanned Aircraft Systems Aviation Rulemaking Committee (ARC), ARC Recommendations Final Report, Apr. 1, 2016.

80 *See* Juan Plaza, Highlights from FAA Administrator Michael Huerta's CES Address, Commercial AUV News, Jan. 24, 2017; Linda Chiem, FAA Chief Says Drone Flight-Over-People Rule Still in Works, Law360, Jan. 6, 2017.

81 FAA, Press Release, FAA Administrator Makes Two Major Drone Announcements, July 1, 2016; *see also* RTCA, Drone Advisory Committee, Terms of Reference, Sept. 1, 2016.

82 RTCA, Drone Advisory Committee Membership – February 2017.

83 The DAC met in September 2016 and January 2017. Two more meetings are scheduled this year. *See* RTCA, Drone Advisory Committee, *at* http://www.rtca.org/content.asp?pl=33&sl=216&contentid=216 (last visited Feb. 13, 2017).

84 PBS News Hour, *supra*. While progress has been made, frustration with the relatively slow pace led the Senate to include a provision in an aviation bill in 2016 that would have required the FAA to authorize drone deliveries within two years, but the House did not pass its own version of the bill due to unrelated issues. *See id.*

85 Samantha Masunaga, New Rules on Small Drones: What You Need to Know, L.A. Times, Aug. 29, 2016.

86 Chiem, *supra*.

87 FAA Aerospace Forecast: Fiscal Years 2016-2036, at 33 (2016).

88 The Future of Commercial Drone Use, Ins. J., Mar. 29, 2016.

89 *Id.* (quoting speech at South by Southwest event in Austin, Texas in March 2016).

90 Selyukh, *supra* (citing analysis by the Association for Unmanned Vehicle Systems International, the industry trade group).

91 *See* Nat'l Conference of State Legislatures, Current Unmanned Aircraft State Law Landscape, Jan. 5, 2017 (providing legislative overviews of state laws enacted each year between 2013 and 2016).

92 Cecilia Kang, F.A.A. Issues Commercial Drone Rules, N.Y. Times, June 21, 2016; Cecilia Kang, F.A.A. Drone Laws Start to Clash With Stricter Local Rules, N.Y. Times, Dec. 27, 2015.

93 *See* Fran Spielman, Drone Regulations Fly With City Council, Nov. 18, 2015.

94 *See* Chicago Municipal Code § 10-36-390(b).

95 *See id.*

96 *See id.* § 10-36-390(d), (e).

97 *See id.* § 10-36-390(c)(1).

98 *See* Spielman, *supra*.

99 Fed. Aviation Admin., Office of the Chief Counsel, State and Local Regulation of Unmanned Aircraft Systems (UAS) Fact Sheet, Dec. 17, 2015.

100 *See id.* at 2-3.

101 *See id.* at 3.

102 *See* Andrew Zimmitti, A Look at Federal Preemption of State Done Laws, Law360, Oct. 25, 2016 (citing cases).

103 Office of the Governor, Edmund G. Brown, Jr., Veto Message, S.B. 142, Sept. 9, 2015.

104 Office of the Governor, Edmund G. Brown, Jr., Veto Message, A.B. 2148, Sept. 29, 2016.

105 Office of the Governor, Edmund G. Brown, Jr., Veto Message, A.B. 2724, Sept. 29, 2016.

106 *Id.*

107 *Id.*

108 David Garrick, San Diego Cracking Down On Drones With New Regulations, San Diego Union-Tribune, Feb. 13, 2017. A violation treated as an infraction would be subject to a $250 fine, and $500 for a second violation within a year. A violation could also be treated as a misdemeanor, subjecting the operator to a fine of $1,000 or six months in jail. *See id.*

109 *See* Zimmitti, *supra*; *see also* Illinois Unmanned Aerial System Oversight Task Force, UAS Recommendations Report 11 (2016) (recognizing that "[l]ocal ordinances, while well-intentioned, are written by those unfamiliar with the nuances and complexities of FAA airspace and operational regulations" and recommending state-level preemption "to complement existing and future Federal preemption").

110 14 C.F.R. § 107.15.

111 *Id.* § 107.23(a).

112 *Id.* § 107.23(b).

113 *Id.* § 107.27.

114 *See* 81 Fed. Reg. at 42,209 (to be codified at 14 C.F.R. § 107.9).

115 *See* 81 Fed. Reg. at 42,174 (citing 14 C.F.R. part 13 and FAA Order 2150.3B, ch. 7, appx. B).

116 *See* Adam Lidgett, FAA, Drone Operator Reach Settlement Over Flights, Law360, Jan. 17, 2017.

117 *See* Fed. Aviation Admin., Press Release, FAA and Skypan International, Inc., Reach Agreement on Unmanned Aircraft Enforcement Cases, Jan. 17, 2017. SkyPan also agreed to work with the FAA to release three public service announcements over the next year to encourage drone operators to learn and comply with FAA regulations. *See id.*

118 *See* Alan Levin, Drone Close Calls, Sightings by Airlines Up Fivefold, FAA Says, Bloomberg, Mar. 28, 2016. Most of the incidents involved "sightings" with little or no chance of an impact. *See id.* There were no reported collisions. *See id.* More recently, the FAA reported several claims of collisions, but was not able to verify any of them and found the incidents involved birds or other items. *See* Alan Levin, Drone-Plane Near Misses, Other Incidents Surged 46% in U.S., Bloomberg BNA, Feb. 23, 2017.

119 *See* Cadie Thompson, Here are the 2 key Features Amazon Revealed About its Delivery Drones, Business Insider, Jan. 19, 2016.

120 *See* Frederick E. Blakelock, Drone Wars: Will the Litigation Awaken, Lexology, Feb. 14, 2016.

121 *See* Restatement (Second) of Torts § 388 (1965) ("One who supplies directly or through a third person a chattel for another to use is subject to liability to those whom the supplier should expect to use the chattel with the consent of the other or to be endangered by its probable use, for physical harm caused by the use of the chattel in the manner for which and by a person for whose use it is supplied, if the supplier (a) knows or has reason to know that the chattel is or is likely to be dangerous for the use for which it is supplied, and (b) has no reason to believe that those for whose use the chattel is supplied will realize its dangerous condition, and (c) fails to exercise reasonable care to inform them of its dangerous condition or of the facts which make it likely to be dangerous.").

122 *See* Restatement (Third) of Torts: Liability for Physical and Emotional Harm § 20 (2009); Restatement (Second) of Torts §§ 519 to 520 (1965).

123 Restatement (Third) of Torts: Liability for Physical and Emotional Harm § 20.

124 *See id.* cmt. e, k.

125 2 W. Blackstone, Commentaries 18 (Lewis ed. 1902); *see also Bury v. Pope*, 1 Cro. Eliz. 118, 78 Eng. Rep. 375 (Ex. 1586) (adopting doctrine).

126 *See* Restatement (Second) of Torts § 822 (1979).

127 *See id.* § 826; *see also id.* §§ 827 (providing factors to evaluate the gravity of the harm, including the extent of harm involved, the character of the harm, the social value of the type of use or enjoyment invaded, the 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), 898 (proving factors to evaluate the utility of the conduct including the social value of the conduct, the suitability of the conduct to the character of the locality, and the impracticability of preventing of avoiding the harm).

128 *See United States v. Causby,* 328 U.S. 256 (1946).

129 *See id.* at 259.

130 *Id.* at 260-61.

131 *Id.* at 266.

132 *See id.*

133 *Id.*

134 *See* Restatement (Second) of Torts § 652B (1977) (emphasis added). A second form of an invasion of privacy claim, publicity given to private facts, requires publication of a matter concerning the private life of another that would be highly offensive to a reasonable person and is not of legitimate public concern. *Id.* § 652D; *see also* Benjamin D. Mathews, Potential Tort Liability for Use of Drone Aircraft, 46 St. Mary's L.J. 573, 586-87 (2015).

135 *See, e.g.,* Fla. Stat. Ann. § 934.50 (authorizing compensatory damages, injunctive relief, attorneys' fees, and potentially punitive damages if a drone is used for surveillance of a person on his or her private property); Tex. Gov't Code §§ 423.001 to 423.006 (prohibiting using drone to capture an image or an individual or privately owned real property with the intent to conduct surveillance and providing a private right of action subject to a civil penalty of $5,000 per episode, $10,000 for distribution of any images captured, or actual damages if distributed with malice).

136 *See* Joshua Briones, Esteban Morales & Natalie Prescott, An Update on Drone Privacy Concerns, Law360, Oct. 5, 2016.

137 *See* Taylor Bilton, When Your Neighbor's Drone Pays an Unwelcome Visit, Jan. 27, 2016.

138 *See* Elisha Fieldstadt, Case Dismissed Against William H. Merideth, Kentucky Man Arrested For Shooting Down Drone, NBC News, Oct. 27, 2015.

139 *See* Andrea Peterson & Matt McFarland, You May Be Powerless to Stop a Drone From Hovering Over Your Own Yard, Wash. Post, Jan. 13, 2016.

140 *Boggs v. Merideth*, No. 3:16-cv-00006-DJH (W.D. Ky. filed Jan. 4, 2016). The defendant filed a motion to dismiss on jurisdiction grounds in March 2016. The docket indicates no activity since June 2016.

141 *See* Andrew Wolfson, Drone-Slayer Suit Could Set US Law, Courier-J., Jan. 14, 2016.

142 Office of the Governor, Edmund G. Brown, Jr., Veto Message, S.B. 142, Sept. 9, 2015.

143 A.B. 856 (Cal. 2015) (amending Cal. Civ. Code § 1708.8).

144 Cal Civ. Code § 1708.8(a) (emphasis added).

145 Cal. Civ. Code. § 1708.8(d).

146 *See* Amanda Fitzsimmons & Monica D. Scott, Drones in California: The Laws, The Proposals, Law360, Mar. 8, 2016.

147 *See* Illinois Unmanned Aerial System Oversight Task Force, UAS Recommendations Report 25-26 (2016).

148 *Id.* at 26.

149 81 Fed. Reg. at 42,183.

150 *Id.*

151 *See* Sean P. Mahoney & Geoffrey F. Sasso, Game of Drones: Liability and Insurance Coverage Issues Coming, Legal Intelligencer, Aug. 29, 2016.

152 *See id.; see also* Nathan Bohlander, Here Come the Drones – And the Legal Headaches, Law 360, Feb. 23, 2017 (noting that specialty insurers, such as the Unmanned Risk Management and Avion Insurance, as well as larger insurers such as AIG, are offering drone insurance to commercial customers); Darren Fishell, How to Prevent Your New Drone from Landing You in Court, Bangor Daily News, Jan. 22, 2017 (including interview with CEO of a new commercial drone insurance startup that offers coverage by the hour to businesses as an alternative to a traditional annual policy).

153 *See* Jayleen R. Heft, 14 Things You Need to Know About Commercial Drones and Insurance, Property Casualty 360, Apr. 28, 2016.

154 *See* Kenneth Chang, SpaceX Launches Rocket Carry Space Station Cargo, N.Y. Times, Feb. 19, 2017.

155 *See, e.g.,* Kenneth Chang, Mike Isaac & Matt Richtel, SpaceX Rocket Explodes at Launchpad in Cape Canaveral, N.Y. Times, Sept. 1, 2016 (reporting 2016 SpaceX explosion that destroyed a $200 million satellite that would have provided internet service to Africa, the Middle East, and Europe, and 2015 explosion of rocket carrying cargo to the International Space Station).

156 *See* General Accounting Office, Federal Aviation Administration: Commercial Space Launch Industry Developments Present Multiple Challenges, GAO-15-706, at 17 (Aug. 2015) GAO Report.

157 Fed. Aviation Admin., The Annual Compendium of Commercial Space Transportation: 2016, at 10 (2016) (FAA 2016 Compendium).

158 Chang, *supra*.

159 *See id.*; *see also* Boeing, CST-100 Starliner, *at* http://www.boeing.com/space/starliner/ (last visited Feb. 21, 2017).

160 *See* GAO Report, *supra*, at 7-9.

161 *See* GOA Report, *supra*, at 7.

162 For several years, Virgin Galactic has accepted full deposits of the $250,000 ticket price for a two-and-a-half hour flight aboard SpaceShip Two, and has reportedly sold at least 640 tickets. *See* Daisy Carrington**,** What does a $250,000 ticket to space with Virgin Galactic actually buy you?, CNN, Aug. 16, 2013.

163 *See* Space Adventures, Space Station, *at* http://www.spaceadventures.com/experiences/space-station/ (last visited Feb. 28, 2017).

164 *See* Kenneth Chang, SpaceX Plans to Send 2 Tourists Around Moon in 2018, N.Y. Times, Feb. 27, 2017.

165 FAA 2016 Compendium, *supra*, at 21.

166 *See generally* Spaceport America, *at* http://www.spaceadventures.com/experiences/space-station/

167 *See generally* Jennifer Hackett, New Law Paves the Way for Asteroid Mining—But Will It Work, Scientific American, Dec. 4, 2015.

168 *See* Mike Wall, Asteroid Mining May be a Reality by 2025, Space.com, Aug. 11, 2015; *see also* Sarah Scoles, Asteroid Mining Sounds, Hard, Right? You Don't Know the Half of It, Wired, Jan. 13, 2017 (reporting that Planetary Resources and Deep Space Industries are putting their technology to use in observing Earth, as they prepare for asteroid exploration).

169 *See* Hackett, *supra*.

170 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, art. VI, Oct. 10, 1967.

171 *Id.* art. VII.

172 *Id.* art. V; *see also* Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space, Dec. 3, 1968 (elaborating on provision of the Outer Space Treaty).

173 Outer Space Treaty, art. III.

174 Convention of International Liability for Damage Caused by Space Objects, Art. I, Mar. 29, 1972, 24.2 U.S.T. 2389, 961 U.N.T.S. 187.

175 Convention of International Liability for Damage Caused by Space Objects art. III–IV.

176 Commercial Space Launch Act of 1984, Pub. L. No. 98-575,§ 2, 98 Stat. 3055, 3055.

177 *Id.*

178 *See id.*

179 *See* General Accounting Office, Federal Aviation Administration: Commercial Space Launch Industry Developments Present Multiple Challenges, GAO-15-706, at 5 (Aug. 2015).

180 Commercial Space Launch Act Amendments of 1988, Pub. L. No. 100-657, § 5(a).

181 51 U.S.C. § 50914.

182 Commercial Space Launch Amendments Act of 2004, Pub. L. No. 108-492, 118 Stat. 3974.

183 *Id.* § 2 (codified at 51 U.S.C. § 50901(a)(11)).

184 *Id.* § 2 (codified at 51 U.S.C. § 50901(a)(12), (14)).

185 *Id.* (codified at 51 U.S.C. § 50901(a)(15)).

186 51 U.S.C. § 50914(a)-(c).

187 51 U.S.C. § 50905(b)(5)(A).

188 *Id.* at § 50905(b)(5)(C).

189 *See* 14 C.F.R. § 460.45.

190 14 C.F.R. § 460.49.

191 Pub. L. No. 112- 95, § 827, 126 Stat. 11, 133 (2012).

192 Pub. L. No. 114-90 (2015).

193 *See id.* § 103 (amending 51 U.S.C. § 50914 and extending operation until September 30, 2025).

194 *See* 51 U.S.C. § 50915(a) (including inflation adjustment).

195 *Id.* § 106, 129 Stat. 707 (codified at 51 U.S.C. § 50914(g)).

196 *Id.* § 115, 129 Stat. 717.

197 *Id.* § 111, 129 Stat. 711 (codified at 51 U.S.C. § 50905(c)(2)(C), (c)(9)).

198 *Id.* § 513, 129 Stat. 721 (codified at 51 U.S.C. §§ 51301 to 51303).

199 *See* Am. Ass'n for Justice, Press Release, Space Act Eliminates Accountability for Private Space Travel Industry, May 13, 2015.

200 *See* Fed. Aviation Admin., The Economic Impact of Commercial Space Transportation on the U.S. Economy in 2009, at 2 (Sept. 2010).

201 *See generally* Fed. Aviation Admin., State Support for Commercial Space Activities (2013) (providing compilation of state incentives).

202 *See* Va. Code Ann. §§ 8.01-227.8 to 8.01-227.10. Virginia also enacted the Zero G Tax Act of 2008, which provides an exemption from state income taxes to any space transportation company doing business in Virginia with the intent to either launch payloads from the Mid-Atlantic Regional Spaceport or conduct spaceflight training.

203 *See* Fla. Stat. Ann. § 331.501.

204 *See* N.M. Stat. Ann. §§ 41-14-1 to 41-14-4 ("Space Flight Informed Consent Act").

205 Tex. Civ. Prac. & Rem. Code Ann. §§ 100A.001 to 100A.004.

206 Cal. Civ. Code § 2212(d).

207 Colo. Rev. Stat. § 41-6-101.

208 Okla. Stat. tit. 3, §§ 3-351 to 3-353.

209 *See* Dave William, Georgia Spaceport Project Hinges on Liability Shield Law, Atlanta Bus. Chron., Aug. 23, 2016.

210 *See* H.B. 734 (Ga. 2016). As introduced, the bill also precluded nuisance claims stemming from spaceflight operators, but this section was removed from the bill.

211 *See* Fahey, *supra* (reporting testimony by Dan Murray and Jared Stout of FAA's Office of Commercial Space Transportation).

212 FAA 2016 Compendium, *supra*, at 8-9.

213 *See* Mark Fahey, When a Rocket Blows Up, Space Insurers Pay for It, CNBC, Sept. 1, 2016.

214 Pub. L. No. 114-90, § 111, 129 Stat. 709-10 (codified at 51 U.S.C. § 50905(c)(3)).

215 *See* ASTM, ASTM Standardization News (Nov.-Dec. 2016).

216 *See* Caley Albert, Liability in International Law and the Ramifications on Commercial Space Launches and Space Tourism, 36 Loy. L.A. Int'l & Comp. L. Rev. 233, 249-54 (2014) (comparing United States program to indemnification system in China, France, and Russia).

217 *See generally* Maria-Vittoria "Giugi" Carminati, Is Statutory Immunity for Spaceflight Operators Good Enough?, 6 Legis. & Policy Brief 35 (2014).

218 *See* Price Waterhouse Cooper, The Sharing Economy (2015).

219 *See* Joel Stein, Baby, You Can Drive My Car, and Do My Errands, and Rent My Stuff…, Time, Jan. 29, 2015.

220 *See* Fed Trade Comm'n, The "Sharing" Economy: Issues Facing Platforms, Participants & Regulators, (Nov. 2016); Rudy Telles, Jr., Digital Matching Firms: A New Definition in the 'Sharing Economy' Space, Dept. of Commerce, June 3, 2016.

221 *See* Molly Cohen & Corey Zehngebot, What's Old Becomes New: Regulating the Sharing Economy, 58 Boston B.J. 6 (2014).

222 *See* Brian Solomon, Uber Just Completed Its Two Billionth Ride, Forbes, July 18, 2016.

223 *See* Alyson Shontell, LEAKED: Internal Uber Deck Reveals Staggering Revenue and Growth Metrics, Business Insider, Nov. 20, 2014.

224 *See id.*

225 *See* Lora Kolodny, Uber Losses Expected to Hit $3 Billion in 2016 Despite Revenue Growth, TechCrunch, Dec. 21, 2016.

226 *See* Brad Stone, The $99 Billion Idea, Bloomberg Technology, Jan. 26, 2017.

227 *See* Mark J. Perry, Top 10 Uber Facts, AEI, June 2, 2014.

228 *See* Erika Fry *et al.*, 25 Most Important Private Companies, Fortune, 2016.

229 *See* Uber and the American Worker Remarks from David Plouffe, Uber Newsroom, Nov. 3, 2015.

230 *See id.*

231 *See* Jonathan V. Hall & Alan B. Krueger, An Analysis of the Labor Market for Uber's Driver-Partners in the United States, NBER Working Paper No. 22843; Geoff Weiss, The Median Income of an Uber Driver in NYC Is Nearly $100,000, Entrepreneur, May 28, 2014; Uber Transportation Network Now Covers 43 Percent of the U.S. Population; Business Wire, May 27, 2014.

232 *See* Jonathan Hall, In the Driver's Seat: A Closer Look at the Uber Partner Experience, Uber Newsroom, Jan. 22, 2015.

233 *See id.*

234 *See* Avery Hartmans, Lyft Lost $600 Million Last Year, But It's Making Progress in its Ride-Hailing War with Uber, Business Insider, Jan. 12, 2017; Eric Newcomer, Lyft Loses $600 Million in 2016 as Revenue Surges, Bloomberg Tech., January 12, 2017.

235 *See id.*

236 Dara Kerr, Lyft Rolls Out to 54 More US Cities in Uber Blitz, CNET, Feb. 23, 2017.

237 Lyft Public Comments on Sharing Economy Workshop, Project No. P15-1200, What is Lyft, Lyft, May 26, 2015.

238 *See* New Report from MADD, Uber Reveals Ridesharing Services Important Innovation to Reduce Drunk Driving, MADD, Jan. 27, 2015.

239 *See* Emily Badger, Are Uber and Lyft Responsible for Reducing DUIs?, Wash. Post, July 10, 2014.

240 *See* Brittany Hunter, Without Uber or Lyft, Austin Experiences Skyrocketing DUI Rates, FEE, Jan 4, 2017.

241 *See* Davey Alba, Uber Cheaper, Faster, More Reliable for Lower-Income Neighborhoods, Wired, July 20, 2015; *see also* Lyft Public Comments on Sharing Economy Workshop, Project No. P15-1200, What is Lyft, Lyft, May 26, 2015.

242 *See* Airbnb, About Us, *at* https://www.airbnb.com/about/about-us (last visited Mar. 20, 2017).

243 *See id.*

244 Rafat Ali, Airbnb's Revenues Will Cross Half Billion Mark in 2015, Analysts Estimate, SKIFT, Mar. 25, 2015.

245 *See* Howard Yu, Marriott and Hilton Stay Ahead of the Sharing Economy, Proving that Airbnb Is Not the Uber of Hotels, Forbes, Feb. 16, 2017; Max Chafkin & Eric Newcomer, Airbnb Faces Growing Pains as It Passes 100 Million Guests, Bloomberg Businessweek, July 11, 2016.

246 *See id.*

247 *See* Airbnb, The Economic Impacts of Home Sharing in Cities Around the World *at* https://www.airbnb.com/economicimpact (last visited Mar. 20, 2017).

248 *See id.*

248 *See* Brad Tuttle, Marriott's CEO Just Made a Pretty Good Sales Pitch for...Airbnb?, Money, July 9, 2014.

250 *See* Tomio Geron, Airbnb Had $56 Million Impact on San Francisco: Study, Forbes, Nov. 9, 2012.

251 *See id.*

252 *See id.*

253 *See* Airbnb's Economic Impact on the NYC Community, *at* blog.airbnb.com/airbnb-economic-impact-nyc-community/ (last visited Mar. 20, 2017).

254 *See id.*; *see also* Laura Kusisto, Airbnb Cites Its Role in City, Wall St. J., Oct. 21, 2013.

255 *See* Airbnb, Host Employment in New Orleans, at 6 (Oct. 2016).

256 *See* Airbnb, The Economic Impacts of Home Sharing in Cities Around the World, *supra.*

257 *See id.*

258 *See* The Rise of the Sharing Economy, Economist, Mar. 9, 2013.

259 *See generally* FTC Staff Report, The "Sharing" Economy Issues Facing Platforms, Participants & Regulators, Nov. 2016; Adam Thierer, Christopher Koopman, Anne Hobson, and Chris Kuiper, How the Internet, the Sharing Economy, and Reputational Feedback Mechanisms Solve the "Lemons Problem," 70 U. Miami L. Rev. 830 (2016); Christopher Koopman, Matthew Mitchell & Adam Thierer, The Sharing Economy and Consumer Protection Regulation, 8 J. Bus. Entrepreneurship & L. 529 (2015); Sofia Ranchordas, Does Sharing Mean Caring? Regulating Inovation in the Sharing Economy, 16 Minn. J.L. Sci. & Tech.413, 462-66 (2015).

260 *See* Details on Safety at Uber, updated May 12, 2016, *at* https://www.newsroom.uber.com/details-on-safety.com; at Lyft, We Go the Extra Mile For Safety, *at* https://www.lyft.com/safety (last visited Mar. 20, 2017).

261 *See generally* Matthew Feeney, Is Ridesharing Safe?, Cato Inst., Jan. 27, 2015.

262 *See* Jason Tanz, How Airbnb and Lyft Finally Got Americans to Trust Each Other, Wired, Apr. 23, 2014.

263 *See* Airbnb, Terms of Service, *at* https://airbnb.com/terms (last visited on Mar. 20, 2017).

264 *See* Jason Tanz, How Airbnb and Lyft Finally Got Americans to Trust Each Other, Wired, Apr. 23, 2014.

265 *See* Kat Greene, Uber Sued Over Death Of 6-Year-Old Girl, Law360, Jan. 27, 2014.

266 *See* Ellen Huet, Uber Rider Might Lose An Eye From Driver's Hammer Attack. Could Uber Be Held Liable?, Forbes, Sept. 30, 2014; Ben Popken, States Warn of Rideshare Risks for Passengers, NBC News, May 28, 2014; Perry Stein, Uber Driver Charged With Sexually Assaulting Passenger in D.C., Wash. City Paper, July 28, 2014.

267 *See* Rebecca Shinners, 10 Airbnb Horror Stories That Will Make You Cringe, Country Living, July 25, 2016; George Hobica, 10 Incredible Airbnb Horror Stories, Fox News, May 8, 2014.

268 *See* Complaint for Damages and Demand for Trial by Jury at 4, *Liu v. Uber Techs., Inc.*, No. CGC-14-536979 (Cal. Super. Ct. Jan. 27, 2014).

269 *See Mazaheri v. Doe*, No. CIV-14-225-M, 2014 WL 2155049, at *2 (W.D. Okla. May 22, 2014).

270 *See id.*

271 *See e.g., Search v. Uber Tech., Inc.*, 2015 WL 5297508 (D.D.C. 2015) (tort victim sufficiently alleged existence of employment relationship between driver and ride-sharing company).

272 *See McGillis v. Uber,* No. 3D15-2758 (Fla. 3 DCA Feb. 1, 2017).

273 *See id.*

274 *See id.*

275 *See O'Connor v. Uber Tech., Inc.*; No. 13-cv-03826-EMc , 2013 WL 4742878 (N.D. Cal. filed Aug. 16, 2013); *Cotter v. Lyft Inc.*, 13-cv-04065 (N.D. Cal. filed Sep. 13, 2013).

276 *See* Tracey Lien, Uber Sued Again Over Drivers' Employment Status, L.A. Times, May 2, 2016 (reporting nationwide employment class actions filed against Uber in Florida and Illinois, following litigation in California and Massachusetts).

277 *See O'Connor v. Uber Tech., Inc.*; (N.D. Cal. 2016) (order denying settlement); Dorothy Atkins, Lyft Nears OK On $27M Wage Deal Amid Driver Objections, Law360, Dec. 1, 2016.

278 *See In re Uber Techs., Inc., Wage & Hour Emp't Practices*, MDL No. 2686, 2016 WL 439976, at *1 (J.P.M.L. Feb. 3, 2016); *Ramos v. Uber Techs., Inc.*, No. SA-14-CA-502-XR, 2015 WL 758087, at *12 (W.D. Tex. Feb. 20, 2015); *Lavitman v. Uber Techs., Inc.*, No. SUCV201204490, 2015 WL 728187, at *6 (Mass. Super. Ct. Jan. 26, 2015).

279 *See Berwick v. Uber Techs., Inc.*, No. 11-46739 EK, slip op. at 8 (Cal. Labor Comm'r June 3, 2015).

280 *See e.g., New Yorkers Making Ends Meet in the Sharing Economy v. Airbnb, Inc.,* No. 158526/2014 (N.Y. Sup. Ct. Oct. 1, 2014); *see also* Johanna Interian, Up in the Air: Harmonizing the Sharing Economy through Airbnb Regulations, 39 B.C. Int'l & Comp. L. Rev. 129 (2016).

281 *See* Ellen Huet, Rideshare Drivers Still Cornered Into Insurance Secrecy, Forbes (Dec. 18, 2014).

282 *See* Uber, Insurance Coverage, Nairi, Insurance for Ridesharing with Uber, Uber Newsroom, Feb. 10, 2014.

283 *See id.*

284 *See* Nat'l Ass'n for Ins. Commissioners, Transportation Network Company Insurance Principles for Legislators and Regulators, NAIC White Paper (Mar. 31, 2015).

285 *See* Allstate to Offer Ridesharing Endorsement in Four States, Ins. J., June 5, 2015; American Family Launches Coverage for Ridesharing Drivers in Colorado, Ins. J., May 21, 2015; Geico Ridesharing Policy Now Available to Connecticut Drivers, Bus. Wire, Sept. 15, 2015; MetLife Expands Ridesharing Insurance Policy to Five States, Including California, Bus. Wire, Oct. 12, 2015.

286 *See* Ron Lieber, A Liability Risk for Airbnb Hosts, N.Y. Times, Dec. 5, 2014; Ron Lieber, Home-Sharing? Don't Ignore Liability, N.Y. Times, Apr. 20, 2002.

287 *See* Airbnb, Host Protection Insurance, *at* https://www.airbnb.com/protection-insurance (last visited Feb. 28, 2017).

288 *See* Airbnb, What Is the Resolution Center?, *at* https://www.airbnb.com/help/article/767/what-is-the-resolution-center (last visited Feb. 28, 2017).

289 *See* Jason Tanz, How Airbnb and Lyft Finally Got Americans to Trust Each Other, Wired, Apr. 23, 2014.

290 *See id.*

291 *See* Austin Carr, The Secret to Airbnb's Freakishly Rapid Orgy Response: "Scenario Planning," Fast Company, Mar. 17, 2014.

292 *See* Tracey Lien, Uber and Lyft Drivers are Safer Than the Average American Driver, According to New Report; L.A. Times, May 26, 2016; Matthew Feeney, Is Ridesharing Safe?, Cato Ins., Jan. 27, 2015.

293 *See* Ann-Marie Alcantara, Study Finds Taxi Drivers Are the Worst Drivers, Bold Italic, Dec. 11, 2014.

294 *See id.*

295 *See* The Sharing Economy Boom and Backlash, Economist, April 25, 2014.

296 *See* Where (and Why) is Rideshare Banned? I Drive with Uber (blog), Mar. 14, 2016 (compiling state laws banning ride sharing); *see also* Katie Collins, Uber Facing More Roadblocks in Cities Around the World, CNET, Sept. 30, 2015; Eva Grant & Simran Khosla, Here's Everywhere Uber Is Banned Around the World, Business Insider Tech., Apr. 8, 2015.

297 *See* Application of Rasier, LLC for a Class C - Transp. Network Co. Certificate of Pub. Convenience & Necessity for Operation of Motor Vehicle Carrier, No. 2014-372-T, 2015 WL 243537, at *2 (S.C. P. Service Comm'n Jan. 15, 2015); *Uber Techs., Inc. v. Second Judicial Dist. Court of State ex rel. Cnty. of Washoe,* No. 66875, 2014 WL 6680785, at *1 (Nev. Nov. 24, 2014); Petition of the Bureau of Investigation & Enforcement of the Pa. Pub. Util. Comm'n for an Interim Emergency Order Requiring Uber Techs., Inc. to Immediately Cease & Desist from Brokering Transp. Serv. for Comp. Between Points Within the Commonwealth of Pennsylvania, No. P-2014-2426846 2014 WL 3763990, at *15, (Pa. P.U.C. July 24, 2014).

298 *See* Celia Ampel, Broward County Votes To Regulate Uber, Lyft as Taxi Services, Bus. J., Feb. 10, 2015; Reid Wilson, Seattle Becomes First City to Cap Uber, Lyft Vehicles, Wash. Post, Mar. 18, 2014.

299 *See* Harriet Taylor, Uber and Lyft are Getting Pushback from Municipalities All Over the US, CNBC, Sept. 2, 2016; *see also* Mike Dingman, Uber's Departure is Anchorage's Loss - and Cab Cartel's Gain, Alaska Dispatch News, June 29, 2016.

300 *See* Cal. Pub. Util. Code § 5432(a); Colo. Rev. Stat. Ann. §§ 40-10.1-601-40-10.1-608.

301 *See* Cal. Pub. Util. Code §§ 5432 - 5436; Colo. Rev. Stat. Ann. §§ 40-10.1-601-40-10.1-608.

302 *See id.*

303 *See* Ariz. Rev. Stat. Ann. §§28-9551-28-9558; Ark. Code Ann. §§23-13-702 - 23-13-722; D.C. Code Ann.§50-301.29; Ga. Code Ann. §33-1-24; Idaho Code Ann. §§41-2517-41-2521; 625 Ill. Comp. Stat. Ann. 57/10; Ind. Code Ann. §8-2.1-19.1;Kan. Stat. Ann. §§8-2708-8-2710; Ky. Rev. Stat. Ann. §281.655; La. Stat. Ann. §§45:201.6-45:201.9; 24-A M.R.S.A. §§7303-7305; Md. Code Ann., Pub. Util. §10-405; Minn. Stat. Ann. §65B.472; Mont. Code Ann. §§69-12-343, 69-12-344; Neb. Rev. Stat. Ann. §§75-333, 75-341; 2015 Nev. Stat. §279; N.C. Gen. Stat. Ann. §§20-280.1-20-280.10; N.D. Cent. Code §§26.1-40.1-01-26.1-40.1.11; Okla. Stat. Ann. tit. 47, §§1025-1030; S.C. Code Ann. §§58-23-1625-58-23-1635; Tenn. Code Ann. §55-12-141; Texas Ins. Code Ann. art. §§1954.001, 1954.052-1954.053, 1954.101; Utah Code Ann. §13-51-108; Va. Code Ann. §46.2-2099.52; Wash. Rev. Code Ann. §48.177.010; Wis. Stat. Ann. §440.48.

304 *See* Gartner, Inc., Press Release, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, Feb. 7, 2017.

305 *See* Jonathan Camhi, BI Intelligence Projects 34 Billion Devices will be Connected by 2020, Bus. Insider, Nov. 6, 2015.

306 *See* Julie Steinberg, Fifty Billion Connected Devices Bring Tort, Software Law Clash, Bloomberg BNA, Feb. 26, 2016.

307 *See* Camhi, *supra.*

308 *See* Harriet Taylor, How the 'Internet of Things' Could be Fatal, CNBC, Mar. 4, 2016 (discussing wireless connectivity of pacemakers and noting that while there are no known cases in which malicious hackers have attacked a pacemaker, researchers say it is possible).

309 *See* McKinsey Global Inst., Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy 56-58 (May 2013) (predicting that IoT will contribute $2.7 to $6.2 trillion to the world economy each year by 2025).

310 *See* Julie A. Steinberg, Fifty Billion Connected Devices Bring Tort, Software Law Clash, Bloomberg BNA, Feb. 26, 2016 (quoting plaintiffs' attorney Steven Teppler of the Abbott Law Firm in Jacksonville, Florida).

311 *See* Craig Timberg, Elizabeth Dwoskin & Ellen Nakashima, WikiLeaks: The CIA is Using Popular TVs, Smartphones and Cars to Spy on Their Owners, Wash. Post, Mar. 7, 2017.

312 *See, e.g.,* Sarah Kellogg, Every Breath You Take: Data Privacy and Your Wearable Fitness Device, Wash. Lawyer, Dec. 2015, at 22 (recognizing that while health information recorded by mobile devices is typically not subject to the Health Insurance Portability and Accountability Act (HIPAA), data breaches are subject to FTC and state attorney general enforcement under unfair and deceptive trade practices laws).

313 *See* 15 U.S.C. § 45(a).

314 *See FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236, 255 (3d Cir. 2015) (holding that cybersecurity practices can form the basis of an unfair practice under the FTC Act).

315 *See* Taylor Armerding, The IoT Liability Jumble, CSO, Mar. 2, 2016 (quoting Nithan Sannappa's comments at an RSA conference titled, "Flaming toasters to crashing cars – the Internet of Things and mass liability").

316 *See* Complaint, *In the Matter of TrendNet, Inc.*, FTC File No. 122 3090, Docket No. C-4426, at 5 (FTC filed Jan. 16, 2014).

317 *See* Decision and Order, *In the Matter of TrendNet, Inc.*, FTC File No. 122 3090, Docket No. C-4426, at 5 (FTC Jan. 16, 2014).

318 Steinberg, *supra* (discussing comments of Steven Teppler).

319 *See* Garner, Press Release, Gartner Says By 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities, Jan. 26, 2015.

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

321 *See* 147 F. Supp. 3d at 958-59.

322 Complaint, *Cahen v. Toyota Motor Corp.*, No. 3:15-cv-01104, at 8 (N.D. Cal. filed Mar. 10, 2015).

323 *See generally id.*

324 *See* 147 F. Supp. 3d at 968.

325 *Id.* at 969.

326 *Cahen v. Toyota Motor Corp.*, No. 16-15496 (9th Cir.).

327 *See* Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway—With Me in It, Wired, July 21, 2015.

328 *See Flynn v. FCA US LLC,* No. 3:15-cv-00855 (S.D. Ill. filed Aug. 4, 2015).

329 *See* Rick Archer, Fiat Rips Suit Over 'Remote Possibility' of Jeep Hack, Law 360, Feb. 6, 2017.

330 *See Flynn v. FCA US LLC*, No. 15-cv-0855, 2016 WL 5341749, at *2 (S.D. Ill. Sept. 23, 2016) (citing *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1147 & n.5 (2013)).

331 *See id.* at *3-4.

332 *See id.* at *8.

333 Dick Cheney's Heart, 60 Minutes, CBS News, Oct. 20, 2013; *see also* Andrea Peterson, Yes, Terrorists Could Have Hacked Dick Cheney's Heart, Wash. Post, Oct. 21, 2013.

334 *See* Muddy Waters is Short St. Jude Medical, Inc. (STJ:US) (Aug. 25, 2016), *at* http://www.muddywatersresearch.com/research/stj/mw-is-short-stj/ (last visited Mar. 2, 2017).

335 Complaint, *Ross v. St. Jude Medical Inc.*, No. 2:16-cv-06465, at 13-15 (C.D. Cal. filed Aug. 26, 2016).

336 *Id.* at 8.

337 *Id.* at 14-15.

338 *See* Shayna Posses, St. Jude Sues Over 'Defamatory' Cardiac Device Report, Law360, Sept. 7, 2016.

339 *See* In Chambers – Order and Notice to Parties, *Ross v. St. Jude Medical Inc.*, No. 2:16-cv-06465 (C.D. Cal. Dec. 28, 2016) (order granting voluntary dismissal without prejudice).

340 *See St. Jude Medical Inc. v. Muddy Waters Consulting LLC,* No. 16-cv-03002 (D. Minn.).

341 *See* Julie Steinberg, Fifty Billion Connected Devices Bring Tort, Software Law Clash, Bloomberg BNA, Feb. 26, 2016 (citing plaintiffs' attorney Steven Teppler of the Abbott Law Firm who is involved in the Barbie and VTech litigation).

342 *See Archer-Hayes v. Toytalk, Inc.,* No. BC603467, 2015 WL 8304161 (Cal. Super. Ct., Los Angeles County, filed Dec. 7, 2015).

343 *See* Jack Newsham, 'Hello Barbie' Doll Records Kids Without Consent, Suit Says, Law360, Dec. 9, 2015.

344 *See* Stipulation of Voluntary Dismissal with Prejudice, *Archer-Hayes v. Toytalk, Inc.*, No. 2:16-cv-2111 (C.D. Cal. filed July 22, 2016) (Dkt. #42).

345 *See* In the Matter of Genesis Toys and Nuance Communications, Complaint and Request for Investigation, Injunction, and Other Relief (FTC filed Dec. 6, 2016).

346 *See generally In re VTech Data Breach Litig.*, Master Case No. 15-cv-10889 (N.D. Ill.).

347 *See* VTech, Press Release, FAQ About Cyber Attack on VTech Learning Lodge, at https://www.vtech.com/en/press_release/2016/faq-about-cyber-attack-on-vtech-learning-lodge/ (last updated Dec. 16, 2016).

348 *See* VTech Electronics North America, LLC's Motion to Dismiss Plaintiffs' Consolidated Amended Complaint, *In re VTech Data Breach Litig.*, Master Case No. 15-cv-10889 (N.D. Ill. filed Apr. 13, 2016) (Dkt. #61).

349 *Id.* at 1.

350 *See* Parties' Joint Report on Status of Mediator, *In re VTech Data Breach Litig.*, Master Case No. 15-cv-10889 (N.D. Ill. filed Jan. 31, 2017) (Dkt #82).

351 *Clapper v. Amnesty Int'l USA,* 133 S. Ct. 1138, 1148 (2013).

352 *Id.* at 1147.

353 *Id.* at 1150 n.5.

354 *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016).

355 *Id.*

356 *See* Restatement (Second) of Torts § 314 (1965) ("The fact that the actor realizes or should realize that action on his part is necessary for another's aid or protection does not of itself impose upon him a duty to take such action.").

357 *See id.* §§ 314A, 344.

358 *See id.* § 448 ("The act of a third person in committing an intentional tort or crime is a superseding cause of harm to another resulting therefrom, although the actor's negligent conduct created a situation which afforded an opportunity to the third person to commit such a tort or crime, unless the actor [defendant] at the time of his negligent conduct realized or should have realized the likelihood that such a situation might be created, and that a third person might avail himself of the opportunity to commit such a tort or crime.").

359 *See generally* Restatement (Second) of Torts § 388 (1965) (requiring warnings only when a risk associated with a product was known or should have been known at the time of sale).

360 *See* Kenneth Ross & J. David Prince, Post-Sale Duties: The Most Expansive Theory in Products Liability, 74 Brook. L. Rev. 963, 965 (2009) (quoting James A. Henderson, Jr. & Aaron Twerski, Teacher's Manual for Products Liability: Problems And Process 159 (6th ed. 2008)).

361 *See id.* at 963-64.

362 Restatement (Third) of Torts: Prods. Liab. §10 (1998).

363 *Id.* § 11.

364 Vincent J. Vitkowsky, The Internet of Things: A New Era of Cyber Liability and Insurance 4 (Seiger Gfeller Laurie LLP, Feb. 2015).

365 *See* S. Res. 110, 114th Cong. (2015).

366 Sponsors of the DIGIT Act, S. 2607, 114th Cong., included Senators Deb Fischer (R-Nebraska), Kelly Ayotte (R-New Hampshire), Cory Booker (D-New Jersey), Brian Schatz (D-Hawaii).

367 *See* Report of the Committee on Commerce, Science, and Transportation on S. 2607, Developing Innovation and Growing the Internet of Things Act, Rep. No. 114-364, at 5 (Sept. 27, 2016).

368 *See id.*

369 *See* S. 88, 115th Cong. (2017).

370 *See* H.R. 686, 115th Cong (2017) (introduced Jan. 24, 2017).

371 *See* The Spy Car Act, S. 1806, 114th Cong. (introduced July 21, 2015).

372 *See* The Spy Car Study Act, H.R. 3994, 114th Cong. (introduced Nov. 5, 2015); H.R. 701, 115th Cong. (re-introduced Jan. 24, 2017).

373 Armerding, *supra* (citing comments by Eric Hibbard, Chief Technology Officer for Hitachi Data Systems); Vincent J. Vitkowsky, The Internet of Things: A New Era of Cyber Liability and Insurance 4 (Seiger Gfeller Laurie LLP, Feb. 2015).

375 *See generally* Federal Trade Comm'n, Internet of Things: Privacy & Security in a Connected World (Jan. 2015).

375 *See id.* at 48-49.

376 See generally Federal Trade Comm'n, Careful Connections: Building Security in the Internet of Things (Jan. 2015).

377 Nat'l Highway Traffic Safety Admin., Cybersecurity Best Practices for Modern Vehicles (Oct. 2016).

378 *Id.* at 5 (citing 49 U.S.C. §§ 30101 et seq.).

379 *See* U.S. Dep't of Homeland Security, Strategic Principles for Securing the Internet of Things (IoT) (Nov. 15, 2016).

380 *Id.* at 13-14.

381 U.S. Food & Drug Admin., Postmarket Management of Cybersecuity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff 27-30 (Dec. 28, 2016) (recommending elements of an effective postmarket cybersecurity program).

382 *Id.* at 12.

383 Erin Bosman et al., FDA Embraces Internet of Things: New Draft Guidance on Postmarket Cybersecurity for Medical Devices, Feb. 23, 2016.

384 Dep't of Commerce, Internet Policy Task Force & Digital Economy Leadership Team, Fostering the Advancement of the Internet of Things (Jan. 2017).

385 *Id.* at 1.

386 *Id.* at 2.

387 *Id.* at 15.

388 *Id.* The public comment period concluded on March 13, 2017. *See* Notice; Extension of Comment Period, The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 82 Fed. Reg. 11,561 (Feb. 24, 2017).

388 Office of the Governor, Edmund G. Brown, Jr., Veto Message, A.B. 2724, Sept. 29, 2016.

390 *Id.*

391 *See, e.g.*, Lisa Ellman, Op-ed, Trump's Freeze on Regulations Could Cause Major Delays for Commercial Drones, The Hill, Jan. 31, 2017.

U.S. CHAMBER
Institute for Legal Reform

202.463.5724 main
202.463.5302 fax

1615 H Street, NW
Washington, DC 20062

instituteforlegalreform.com