Smart Products: Evolving Liability and Coverage Issues

Product Liability Perspective

Robert G. Smith
Lorance & Thompson, P.C.
2900 North Loop West, Suite 500
Houston, TX 77092

2017 IADC Annual Meeting

Tuesday, July 11, 2017, 8:45-10:15 a.m.

"Connected cars," which are on the road today, merge the driver's digital world and means of transport. Self-driving vehicles, still years away, hold the potential to revolutionize the way people and goods move around. Smart products challenge traditional ideas of tort and product liability and the insurance coverage should apply, loom as the cyber criminal's new frontier, and pose privacy challenges. This panel will explain these phenomenon, explore regulatory challenges, potential litigation frontiers, and insurance industry responses.

Products we use every day are getting smarter with more functions and performance with less consumer input, everything from an internal medical device that is programmable remotely, a refrigerator that tells your mobile phone when it is out of milk, to cars that drive and park themselves. These products are "smart" but they introduce a new world of liability and coverage issues for manufacturers, insurance carriers, and owners and operators of the products.

I. What are "smart products"?

A. Internet of things and smart objects

The Internet of Things (IoT) is the network of physical objects—devices, vehicles, buildings and other items embedded with electronics, software, sensors, and network connectivity—that enables these objects to collect and exchange data. Each thing is uniquely identifiable through its embedded computing system but can interoperate within the existing Internet infrastructure.

A Smart Object is an object that enhances the interaction with not only people but also with other Smart Objects. It can not only refer to interaction with physical world objects but also to interact with virtual (computing environment) objects.

Wikipedia, The Free Encyclopedia

The number of internet-connected devices outnumbered the human population in 2008, reached 13 billion in 2013, and experts estimate the IoT will consist of 50 billion objects by 2020, generating more than $8 trillion in global revenue.

The President's National Security Telecommunications Advisory Committee's (NSTAC) Report to the President on the Internet of Things (November 19, 2014).

B. Why do we want smart products?

Smart devices are more efficient and more reliable because they can self-report problems before they occur. They are usually intelligent and can perform functions adaptively in collaboration with other devices and applications based on programming or on data collected from users and/or the physical world.

Smart products also create large amounts of "data exhaust" that can reveal insights into the consumer (biometrics, location, preferences), all of which amounts to big data that

may be used for helpful or hurtful purposes. It will likely be difficult for manufacturers to avoid becoming dependent on functions and information provided by smart products.

On September 10, 2015, the Federal Bureau of Investigation posted a warning of IoT risks, including vulnerabilities of business and individual data, and possible "compromising the IoT device to cause physical harm."

C. Smart products can be risky

The connection of billions of objects and transfer of data between them creates risk, new vulnerabilities, particularly where a device can be accessed remotely, operated remotely, and/or remotely accessed to change or delete data. Increasing the number of smart products increases the surface area of attack, because each connection is potentially vulnerable.

A 2014 study by Hewlett-Packard found over 90% of all smart devices collected at least one piece of personal information, over 80% failed to use sufficient authentication, and 70% of the tested devices used no encryption when transmitting data.

A smart device can have a technological failure, which may be harmless, but may be critical. In 2015, two security researchers used software to remotely take control of a Jeep Cherokee on the highway.

Many devices are connected in their default state (with no password or default password) and are subject to security breaches. For example, a printer connected to your office network may be connected using default settings. Assuming a vehicle has a good security setting, if you connect a phone with no security to the vehicle, it may create an opportunity for a security breach.

D. Self-driving vehicles

Removing human error and emotion from driving could reduce the number of fatal traffic accidents by 90%. Four of the 48 driverless cars in California were involved in accidents over a six-month period, and a human was at fault in all four accidents.

KPMG issued a white paper in October 2015 suggesting autonomous cars could reduce the number of accidents per vehicle 80% by 2040.

II. Product design issues

A. Customer contact

Manufacturers must maintain closer ongoing relationships with their customers. Consider how car makers currently reach out to customers regarding recall issues by sending letters, posting notices on their websites, newspapers, etc. It will be even more

important that auto manufacturers regularly contact customers or, more specifically, contact their vehicles to update software that controls steering and crash avoidance systems. Software updates must work with vehicles of multiple year models.

Software updates can be done automatically when the vehicle is connected to the internet. However, some States may consider automatic software updates from the manufacturer to the customer to be a violation of their dealership statute.

Hardware updates may be even more problematic. Consider the public reaction when Apple removed the headphone jack from the iPhone 7. The public may agree to purchase a headphone jack adapter to accommodate the design change but significant modifications to a car or truck may not be as easy to implement. For example, what if state of the art design one year includes twelve sensors around the vehicle but five years later most vehicles have thirty sensors?

If a software update is not automatic and the car owner fails to install the update, causing a crash, then liability must be apportioned between the manufacturer for failing to distribute the software update in the best fashion (*i.e.* automatically) and the vehicle owner for failing to install the software update when available.

B. Interoperability

It will likely be important for self-driving vehicles to be able to communicate with each other and with their environment to maximize the safety benefits. It will be critical that vehicle systems be interoperable, meaning they are able to connect with each other and their environment, and communicate data in a form and format that can be understood and is agnostic as to the hardware or software that processes the data.

III. Liability and legal issues

A. Who is the driver?

On February 4, 2016, the National Highway Transportation Safety Administration's (NHTSA) issued a response to Google's (the self-driving car program is now a standalone subsidiary called Waymo (new way forward in mobility)) request for interpretation of several provisions in the Federal Motor Vehicle Safety Standards (FMVSSs) regarding applicability to the Waymo self-driving vehicle. The Waymo vehicle is controlled exclusively by the Waymo Self-Driving System (SDS). As of 2016, Waymo vehicles have self-driven well over 2 million miles, plus an additional 1 billion miles in simulation just in 2016!

Many of the FMVSSs require certain features be located near the driver's seating position (turn signal lever, brake pedal, emergency brake, etc.). As a starting point, the NHTSA determined the Waymo SDS is the "driver," and not any of the vehicle's occupants.

Based on the NHTSA's agreement that the Waymo SDS is the driver, the NHTSA interpreted many of the regulations requiring controls and indicators such that they need not be located where they are available to human occupants of the vehicle. In fact, Waymo argues having controls operable by a human occupant could negatively affect safety. However, because the NHTSA has no way to conduct testing to confirm compliance with the regulations, it could not conclude Waymo's vehicle complied. Regulations must be revised, but in the meantime the author invited Waymo to petition the Agency for exemption from requirements as applicable.

B. Who is liable in an accident?

- Vehicle owner
- Vehicle occupant
- Manufacturer
- Software designer, programmer
- Software hacker
- Governmental agency related to technology that supports self-driving vehicles (internet bandwidth, or other communication problem)

Defending strict liability claims will require a showing of what steps were taken to ensure the safety of the vehicle and the remote operating system. Suits against remote controlled airplane manufacturers, that considered whether the remote driving system caused the incident, are instructive.

A negligence claim may involve whether the vehicle's owner (who may not be present at the time of the accident) timely updated the vehicle's software or maintained the hardware.

Self-driving vehicles will have components such as cameras, sensors, GPS-tracking, software to control acceleration, braking, calculate upcoming obstacles and avoidance maneuvers, the list is endless. Think of all the decisions we make when driving, and the goal is to perfect decision making and driving process. A February 2013 press release by the NHTSA suggested vehicle to vehicle communication will help eliminate many crashes by exchanging data such as speed and position ten times per second.

The Department of Defense funded research to combat potential cyber-attacks on remote vehicle systems. Researchers at the University of Virginia remotely hacked into the control system of a driverless vehicle, and easily controlled the automatic braking, acceleration, and other automatic features of the vehicle.

Depends on the amount of control

There are different levels of control for self-driving vehicles. There have been and are currently vehicles with a variety of increasingly sophisticated operator assistance options (cruise control that slows down automatically when approaching another vehicle andparallel parks on its own). There are vehicles that are self-driving yet have

operator controls. Lastly there are vehicles designed to be self-driving and do not have a steering wheel, foot pedals, or other human controls.

In May 2013, the NHTSA issued its *Preliminary Statement of Policy Concerning Automated Vehicles*, and defines five levels of vehicle automation:

> No-Automation (Level 0): The driver is in complete and sole control of the primary vehicle controls – brake, steering, throttle, and motive power – at all times.
>
> Function-specific Automation (Level 1): Automation at this level involves one or more specific control functions. Examples include electronic stability control or precharged brakes, where the vehicle automatically assists with braking to enable the driver to regain control of the vehicle or stop faster than possible by acting alone.
>
> Combined Function Automation (Level 2): This level involves automation of at least two primary control functions designed to work in unison to relieve the driver of control of those functions. An example of combined functions enabling a Level 2 system is adaptive cruise control in combination with lane centering.
>
> Limited Self-Driving Automation (Level 3): Vehicles at this level of automation enable the driver to cede full control of all safety-critical functions under certain traffic or environmental conditions and in those conditions to rely heavily on the vehicle to monitor for changes in those conditions requiring transition back to driver control. The driver is expected to be available for occasional control, but with sufficiently comfortable transition time. The Waymo car is an example of limited self-driving automation.
>
> Full Self-Driving Automation (Level 4): The vehicle is designed to perform all safety-critical driving functions and monitor roadway conditions for an entire trip. Such a design anticipates the driver will provide destination or navigation input, but is not expected to be available for control at any time during the trip. This includes both occupied and unoccupied vehicles.

There will be disputes over whether an accident is caused by human error or technological failure. The fact-finder will most likely consider whether the occupant could/should have taken over control and avoided the accident.

C. Product defect or negligence?

It is likely whenever self-driving vehicles start operating on the road that human-controlled vehicles will be operating at the same time.

As vehicles progress towards autonomous operation, lawsuits related to accidents will likely move from negligence towards product liability focused actions. Courts will have to determine what is a state of the art vehicle design. A self-driving vehicle cannot be

perfect, but will it be considered reasonably safe if it is safer than an ideal human driver, as safe as the vehicles made by its competitors, or if its incidence of failures is less than a predetermined statistical average of accidents per mile travelled? Manufacturers will have to document how and why they make design decisions so they can prove their vehicles are state of the art.

If self-driving vehicles rely on information exchanged with street signs, the road itself, and other vehicles, apportioning responsibility will be even more complicated. If the vehicle is hacked, the manufacturer may be liable for not having adequate security, but a state of the art vehicle could have an accident based on data received from another vehicle that has been hacked and drawing the lines of liability may not be as simple as with two human drivers.

D. Tesla's Model S Autopilot feature

From Tesla's website:

> "Autopilot allows Model S to steer within a lane, change lanes with the simple tap of a turn signal, and manage speed by using active, traffic-aware cruise control. Digital control of motors, brakes, and steering helps avoid collisions from the front and sides, as well as preventing the car from wandering off the road. Model S can also scan for a parking space, alert you when one is available, and parallel park on command."

Autopilot is designed to assist the driver. If the software failed and despite the driver's input, the car ran off the road, one could argue Tesla was negligent or liable for a product liability action. When the driver's action contributes to the accident, because he failed to react and provide input in time, you can make the argument the driver was negligent or that Tesla's Autopilot feature lulled the driver into a false sense of security.

When an accident involves a design defect and operator misuse, a foreseeable misuse is not an intervening cause that relieves the manufacturer from liability. From Tesla's website:

> "Tesla's commitment to developing and refining the technologies to enable self-driving capability is a core part of our mission.
> …
> Tesla Autopilot relieves drivers of the most tedious and potentially dangerous aspects of road travel. We're building Autopilot to give you more confidence behind the wheel, increase your safety on the road, and make highway driving more enjoyable. While truly driverless cars are still a few years away, Tesla Autopilot functions like the systems that airplane pilots use when conditions are clear. The driver is still responsible for, and ultimately in control of, the car."

Shortly after Autopilot was released a group of drivers drove the Model S across the country, 2,994 miles in 57 hours (including charging time), using Autopilot 96% of the

of the time, at speeds averaging 90 mph. Tesla founder Elon Musk tweeted, "[c]ongratulations on driving a Tesla from LA to NY in just over two days!"

Using Tesla's autopilot feature, driver attention and input is **necessary** for safe use, but is not **required**. Possible misuse is acknowledged on the company's website.

IV. Current and forecasted laws

A. Federal Automated Vehicles Policy

The U.S. Department of Transportation issued the Federal Automated Vehicles Policy in September 2016. The policy includes the following sections:

- Vehicle Performance Guidance for Automated Vehicles
- Model State Policy
- NHTSA's Current Regulatory Tools
- New Tools and Authorities

Manufacturers must submit a Safety Assessment to the NHTSA's Office of the Chief Counsel for each vehicle system, outlining how they are meeting the policy at the time their product is to be ready for testing or deployment on public roads. The Safety Assessment would assist the NHTSA, and the public, in evaluating how safety is being addressed by manufacturers and others developing and testing vehicle systems.

The Safety Assessment would cover the following areas:

- Data Recording and Sharing
- Privacy
- System Safety
- Vehicle Cybersecurity
- Human Machine Interface
- Crashworthiness
- Consumer Education and Training
- Registration and Certification
- Post-Crash Behavior
- Federal, State, and Local Laws
- Ethical Considerations
- Operational Design Domain
- Object and Event Detection and Response
- Fall Back (Minimal Risk Condition)
- Validation Methods

The policy requires manufacturers have a documented process for testing, validation, and collection of event, incident, and crash data, for the purposes of recording the

occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any such issues.

Manufacturers' privacy policies and practices should ensure:

- Transparency
- Choice
- Respect for Context
- Minimization
- Data Security
- Integrity and Access
- Accountability

The policy recognizes vehicle cybersecurity issues are evolving and "more research is necessary before proposing a regulatory standard," manufacturers are encouraged to design vehicle systems following best practices for cyber physical vehicle systems, incorporating "guidance, best practices, and design principles published by National Institute for Standards and Technology (NIST), NHTSA, SAE International, the Alliance of Automobile Manufacturers, the Association of Global Automakers, the Automotive Information Sharing and Analysis Center (ISAC)22 and other relevant organizations."

B. Who should be allowed to "drive" a self-driving vehicle?

1. Several states, including California, District of Columbia, Florida, Michigan, Nevada, and North Dakota, have enacted legislation permitting testing and/or operation of self-driving vehicles under certain conditions.

2. Some states have proposed all self-driving vehicles must have a licensed driver behind a physical steering wheel, which would mean only a person who can pass a driving test could "operate" a self-driving vehicle.

   With such a law, blind and many disabled people could not take advantage of driverless vehicles.

C. What will an auto insurance policy look like?

Legislation passed in California requires driverless vehicle manufacturers to obtain a minimum of $5 million in liability insurance. Manufacturers should anticipate shifting regulations, develop compliance programs, and review their safety testing as the technology evolves.

Insurance policies evolve as well. Early references to cyber liability usually involved an exclusion to coverage. Cyber liability policies next were included as endorsements on general liability policies, and now there are many types of free-standing cyber liability policies.

Volvo, Google, and Mercedes-Benz have issued public statements they will accept full liability if their self-driving vehicles cause an accident. Manufacturers expect the accident rate to go down.

As the risk of accidents goes down, the cost of traditional auto insurance should go down as well, but the manufacturers' cost for product liability insurance will likely go up significantly.

Auto insurance carriers will need to include coverage against cyber-attack, digital interference, and software failure. Proposed legislation in the United Kingdom, the Vehicle Technology and Aviation Bill, would require insurance companies to offer two types of insurance, for when the vehicle is acting autonomously and when the human driver is controlling the vehicle. The legislation includes exemptions from coverage where the vehicle owner makes unauthorized changes to the vehicle's software or fails to install software updates.

Auto insurers will likely seek subrogation from vehicle manufacturers where an accident may be caused by a product design defect, manufacturing defect, or warning defect, etc. Pricing insurance for self-driving cars may be difficult because there is not yet a large body of data on underwriting and losses.

D. New considerations:

1. A driver's license may not be necessary for occupants of a self-driving vehicle.
2. It may not matter if the occupants are intoxicated.
3. What if the occupant is disabled, or blind?
4. Depending on how autonomous the car is, the human occupant may or may not have a duty to intervene if they realize the operating software is malfunctioning or an accident is imminent.
5. The standard for self-driving vehicles could be higher than for a human driver. For example, one could argue the vehicle operating system should recognize that another vehicle is not likely to stop at a red light and should have stopped to allow for the other vehicle's mistake.