Smart Products Require Smarter Manufacturers

2019 IADC Annual Meeting

Thursday, July 11, 2019, 10:30 am to 12:00 noon

Robert G. Smith, Jr.
Lorance Thompson PC
2900 North Loop West, Suite 500
Houston, TX 77092
E-mail: rgs@lorancethompson.com

Chris S. Egner
Global Expert Team - Product Liability / Product Integrity
Continental Corporate Law Department
1830 MacMillan Park Dr.
Fort Mill, SC 29707
E-mail: Chris.Egner@continental.com

Alexandra Simotta
SIX Payment Services (Europe) S.A.
Austrian Branch
Marxergasse 1B,
Vienna, 1030
Austria
E-mail: alexandra.simotta@six-group.com

Louis Charette
Lavery
Suite 4000
1 Place Ville Marie
Montreal QC H3B 4M4
Canada
E-mail: lcharette@lavery.ca

Smart products collect data from their surroundings and from customer input to give feedback to the user and increase the products' usefulness, whether it is speed of travel, distance, heart rate, driving route, or food consumed throughout the day. With these additional data-driven features there is greater risk of cyber security breach that can compromise the confidentiality, integrity, and availability of user data. The massive amount of data collected about all of us can be used for countless things both intended and unintended. For example, information collected by a fitness band could be used to establish rates for health care insurance. In China, data about every aspect of a person's life is being used to establish social credit scores that are used to reward or punish people. If your dog is off the leash or causes a disturbance it could result in losing points, and if enough points are lost the government may confiscate your dog.

Increasing customer demand for smart features that require collection and use of customer data continues to push back against expectations of privacy and requirements for data security. Manufacturers face new challenges to create products that include new smart features that must comply with new and evolving legal and regulatory standards around the world regarding how such data can be legally collected, used, and stored.

Why Smart Products?

Smart products use data to enable features that track a user's progress, report measurements of time or distance, and countless other things. Such products may collect user information on an ongoing basis and help a manufacturer maintain an ongoing relationship with its customers. Depending on the features at issue, a manufacturer can also create features that collect data and provide additional features based on a subscription model which results in an ongoing income stream after the original product sale. Of course, the ongoing relationship can also make it easier to update the product and avoid product failures.

In 2016 the United States National Highway Traffic Safety Administration ("NHTSA") set out a goal of zero traffic deaths. In the United States, almost all motor vehicle accidents are caused by human error with an annual cost of several hundred billion dollars. It is predicted that autonomous vehicles ("AV") will significantly reduce the number of accidents.

While AV technology has evolved rapidly, improvements to the infrastructure (highways, road signs, and bridges, etc.) around the vehicles will exponentially improve overall safety and performance. The "smart" features of an AV are enhanced through accurate interaction with its environment.

An AV's technology can sense its environment alone, but with feedback and input from its surroundings an AV can do much more. For example, using current technology a driver may know the car ahead of them is turning because a turn signal is blinking. An AV may know several blocks before reaching the intersection that a car is turning left in front of it based on data gathered and transmitted by infrastructure in the intersection. AVs may share their entire driving route ahead of time, making turns, stops, and traffic burden much more predictable.

Obviously, significant technological improvements to infrastructure is a long-term process and requires collaboration among public and private entities. The design requirements for public infrastructure must be developed to account for long-term technological changes and improvements.

While software updates are relatively easier to implement, significant upgrades to hardware in the infrastructure or AVs are much more difficult. For example, if the standard autonomous car includes sixteen sensors around the vehicle to establish its position and identify other vehicles, it

is a significant issue if four years after the car is sold the standard is to require sixty sensors on a vehicle.

Consider what statutes and regulations apply

The regulatory structure applicable to smart products and AVs, in particular, can differ dramatically from one state to another and across the world. These differences make it more difficult to create new products that much meet such an array of standards. This creates a significant incentive for manufacturers and creators of new technology to work together alongside governmental agencies to create consistent standards that will maximize the usefulness of smart products and allow companies to focus their research efforts on new useful features.

There is no national consumer privacy statute in the United States, and various state statutes differ quite a bit. The Texas Identify Theft and Protection Act requires businesses that store "sensitive personal information" must implement and maintain reasonable procedures in their related corrective action plan to protect against use or disclosure of sensitive personal information that it collects and maintains and must destroy such information that it should no longer retain. "Sensitive personal information" includes unencrypted first name or first initial and last name in combination with one or more of the following: Social Security Number, driver's license or ID number; account number or credit card number in combination with any required password that would permit access to an account; or information that identifies an individual and their physical or mental health condition, health care provided to them, or payment for health care. The Texas statute creates a private cause of action if personal information is released through a data breach.

The California Consumer Privacy Act of 2018 is quite strict and applies to any company doing business in California with gross revenues over twenty-five million; buys, receives, or sells personal information of 50,000 or more devices, households or consumers; or derives 50% or more of its annual revenue selling personal information. The California statute provides consumers the right to access their data, have their data deleted, and prevent their data from being sold. The statute becomes effective in 2020.

Manufacturers will likely find it burdensome to keep up with numerous differing state statutes in the U.S. and a comprehensive federal law, similar to the GDPR, would likely make compliance simpler.

In September 2018 California passed a new law regarding the security of internet connected devices, the first such statute in the United States. The statute does not become effective until January 1, 2020 but requires manufacturers of connected devices to include reasonable security features to protect stored and transmitted information to prevent access, destruction, use, modification or disclosure. Importantly, most internet connected devices (smart TVs, thermostats, bicycle computers, etc.) are much less secure than your mobile phone or laptop computer. Most such devices do not require a log in or entry of a password and do not include software that can be updated. The statute includes that the connected device must include security features appropriate to the nature and function of the device, appropriate to the information it may collect, store, or transmit, and must be designed to protect the device and the information contained from unauthorized access, destruction, use, modification, or disclosure. If the device is equipped with a means of access from outside a local area network, the security features will be deemed reasonable if the pre-programmed password is unique to each device manufactured or it contains a security feature that requires a user to generate a unique means of authentication before access is granted for the first time.

This California statute regarding internet connected devices applies to smart products that collect, store or transmit "any information," which could include consumer information, business information, user preferences, most any type of data that could be stored. More devices collect data than we often think about. For example, Affinity Health Plan experienced a cyber security breach in 2010 related to thousands of health care records that were stored on hard drives of photocopiers that Affinity leased. The machines were returned to the service provider without removing health care information for 344,000 people from the hard drives. Because of this oversight, Affinity paid a $1.2 million-dollar civil penalty to the U.S. Department Health & Human Services in a 2013 settlement in addition to finding the machines to delete the data and developing a new security plan.

In the U.S., an AV manufacturer could argue that implied preemption of federal law applies, specifically the idea of conflict preemption, where compliance with both federal and state law is impossible or compliance with state law interferes with the objectives of federal law.

The NHTSA regulates motor vehicles while states are responsible for regulations regarding drivers, vehicle licensing, and other rules of operation. The NHTSA issued the Federal Automated Vehicles Policy in 2016 with the goal of establishing a national policy regarding AVs and establishing that the NHTSA alone will regulate the area so there will not be divergent and inconsistent state laws.

In 2017 the NHTSA updated its policy and clarified its non-regulatory position on AVs. The NHTSA's 2018 policy supplements the policy from 2017 and sets out that the NHTSA has authority to establish federal safety standards for vehicles, to address safety defects in vehicles, and no state or local governmental entity may enforce a law regarding safety or equipment on vehicles that differ from federal standards.

The NHTSA has taken a relatively light-handed approach to regulating AVs, which is helpful in an area where the technology is rapidly evolving and improving and encourages continued improvements. Where a federal agency, such as the NHTSA, expressly states that it does not require specific technological features but wants manufacturers to have flexibility in developing and improving various technologies, or that an area should be left unregulated, a defendant may argue a state lawsuit is preempted by federal conflict preemption.

The U.S. House of Representatives passed the Self-Drive Act in 2017 that would preempt state laws regarding the design, manufacture or performance of AVs. Such authority would remain with the NHTSA while the states would oversee licensing and registration, training and insurance issues. A bill in the U.S. Senate, the AV Start Act, would preempt state or local regulation of AV driving systems, set out parameters for testing and evaluation, and pertinent safety parameters. The AV or automated driving system manufacturer would be required to prepare a written plan for identifying and reducing cyber security risks. That neither bill has become law may be a sign of how hard it is to create legislation that maximizes the benefits and minimizes the risks of AVs while the technology is changing so rapidly.

Despite the variety of laws in the U.S., AVs are being tested in several states already, including Texas. Kroger grocery stores are already using unmanned AVs to deliver groceries, through a partnership with Nuro, a technology company founded in 2016 by Google engineers, and its autonomous car is built explicitly for the purpose of transporting goods rather than people.

The French Data Protection Authority imposed a fifty million euro fine against Google on January 21, 2019 which is the first decision issued in France under the General Data Protection Regulation (GDPR) that became law in May 2018. The large majority of the companies (up to 80% in the United States, United Kingdom, and European Union) that are required to comply with

the GDPR are not yet fully compliant. The EU regulatory authorities responsible for enforcing the GDPR also are not ready.

Many smart devices will be subject to the GDPR which regulates a data subject's location in the EU, but only if it is personal data of a natural person. The GDPR applies to a business that offers goods and services to EU residents (even without payment), monitors EU data subjects' behavior within the EU, or processes data in a non-EU country where the GDPR is applicable because of another public international law. Manufacturers must determine whether the GDPR applies to them and their products and if so, take inventory of all types of data collected, where it is stored, and what is done with the data. These steps are necessary to meet the GDPR's requirements that data subjects have a right to request a copy of their data, to confirm whether their data is being processed, and to request their data be erased, or "forgotten."

As artificial intelligence continues to become more robust, regulatory authorities must figure how to regulate systems that are autonomous and make self-directed decisions. The European Parliament adopted a resolution in February 2017 that includes a request that the European Commission submit a proposal that would create a separate legal status for robots such that some robots could be considered "electronic persons." This has been questioned as unreasonable by many legal commentators and political and industry leaders. Giving legal status to robots seems like a bad idea, in such a system it is not impossible to imagine a situation where a robot could have a right superior to a human.

The European Commission issued the Ethics Guidelines for Trustworthy AI on April 8, 2019, which focuses on maximizing the benefits and minimizing the risk of artificial intelligence and includes that trustworthy AI has three components which should be met throughout the system's entire life cycle:

1. It should be lawful, complying with all applicable laws and regulations;
2. It should be ethical, ensuring adherence to ethical principles and values; and
3. It should be robust, both from a technical and social perspective, since, even with good intentions, AI systems can cause unintentional harm.

European Commission's Ethics Guidelines for Trustworthy AI, page 5.

The guidelines also set out seven requirements that AI systems should meet in order to be deemed trustworthy:

1. Human agency and oversight - Including fundamental rights, human agency and human oversight;
2. Technical robustness and safety - Including resilience to attack and security, fall back plan and general safety, accuracy, reliability and reproducibility;
3. Privacy and data governance - Including respect for privacy, quality and integrity of data, and access to data;
4. Transparency - Including traceability, explainability and communication;
5. Diversity, non-discrimination and fairness - Including the avoidance of unfair bias, accessibility and universal design, and stakeholder participation;
6. Societal and environmental wellbeing - Including sustainability and environmental friendliness, social impact, society and democracy; and

7. Accountability - Including auditability, minimization and reporting of negative impact, trade-offs and redress.

European Commission's Ethics Guidelines for Trustworthy AI, page 14.

These seven requirements are relatively subjective, who decides how accountable a robot should be? An AI system is only as trustworthy as the people who created the system, based on their standards for trustworthiness.

The Canadian Centre for Cyber Security was created as of October 2018 and works to consolidate cyber security under one organization. The goals of the CCCS include informing Canadians about cyber security matters, protecting their cyber security interests, developing and distributing cyber security technology, providing cyber security for public assistance, and developing collaboration with private industry. The Canadian Cyber Threat Exchange is a major collaboration between the Canadian government and private industry for sharing information and tactics regarding cyber security threats, intelligence, and technology. In mid-2018 the Canadian government committed over five hundred million dollars to support cyber security projects over the next five years.

Private companies in Canada are subject to mandatory breach notification requirements as of November 1, 2018, as required by the Personal Information Protection and Electronic Documents Act.

It is critical for attorneys to keep up with the evolution of technology and the related new functions, risks, and liabilities. The Texas Disciplinary Rules of Professional Conduct, Rule 1.01, Competent and Diligent Representation, instructs that a lawyer should not accept or continue employment in a legal matter that is beyond the lawyer's competence, and Comment 8 notes that part of maintaining competence is that attorneys should "strive to become and remain proficient and competent in the practice of law, including the benefits and risks associated with relevant technology." This is an increasingly difficult task given that technology evolves exponentially faster than the law. Organizations such as the IADC that aggregate information about developing areas of the law are a great resource for ongoing legal education.

Liability considerations

As smart technology becomes more prevalent new liability theories will be developed. In 2008, a driver filed a lawsuit after being broadsided in an intersection alleging the other driver's Nissan Rogue was unreasonably dangerous and defective because the vehicle did not have automatic braking technology or otherwise warn the driver of an impending collision, alleging such technology should be standard accessories. It is easy to foresee lawsuits alleging all vehicles should have automatic braking technology.

Smart products will likely require more post-sale warnings and product recalls. In many jurisdictions a manufacturer or supplier may be responsible to issue post-sale warnings or to recall or repair products after the sale. The standard under the *Restatement (Third) of Torts* includes that a seller may be liable for failing to provide a warning after sale of the product if a reasonable person in their position would provide such a post-sale warning, taking into consideration whether the seller knows or should know the product poses a substantial risk of harm, whether those who should be warned can be identified and are likely to be unaware of the risk, whether a warning can be effectively communicated to such persons, and whether the risk of harm is sufficient to justify

the burden of providing a warning. Given how many smart products gather customer information on an ongoing basis, it is obviously more difficult for a manufacturer to claim it cannot identify their customers who should receive warnings, and in the case of a recall, a seller can be liable if it fails to act reasonably in recalling a product.

What is reasonable in providing an effective post-sale warning becomes an increasingly daunting hurdle. Smart features also increase the likelihood that a manufacturer will learn of post-sale problems and accidents. Smart technologies make it very difficult for a manufacturer to remain ignorant of post-sale risks that result from a design problem or interaction with new infrastructure or other products.

Smart products generally have varying degrees of ability to respond to external inputs. Very advanced products are said to have "artificial intelligence" but the "intelligence" still derives from algorithmic programming rather than through independent decision-making. Smart products only act or "make decisions" in accord with their design and programming. As such, when a smart product causes injury or damages it can result in liability on behalf of the product manufacturer, such as an allegation that the product failed to incorporate trustworthy AI. If a smart product had artificial intelligence that could make independent decisions it would raise questions about whether the manufacturer could be responsible for problems caused by the independent decisions of such a product.

While the performance of a smart product or its data security failures can lead to manufacturer liability, the data collected by various smart products can be a significant tool in defending a lawsuit because most everyone uses multiple smart products every day. Information collected by and entered into devices such as fitness bands, sports apps on a smart phone, or GPS tracking and other data collected by a car can be used to confirm or contradict testimony related to injuries or other relevant issues.

It is likely that liability issues will be raised regarding how aggressively a manufacturer continues monitoring its smart products, anticipates performance or safety issues, and affirmatively acts to avoid problems.

Products with smart features that require cyber security necessarily require insurance coverage beyond the traditional individual liability policy that covers property damage and personal injuries to the other party. The cost to manufacture, the sale price, and cost of ownership of smart products should incorporate the cost of cyber security insurance coverage. There are unanswered questions about the numerous ways this may be addressed. There will be additional focus on the product manufacturer for questions about the design and manufacturing, and because this is traditionally thought of as the deeper pocket.

Liability claims related to AV accidents may become increasingly complex. Claims could easily involve a blend of strict product liability and negligence, with disputes regarding potential liability of the manufacturer, driver, and vehicle owner. For example, if an autonomous car is involved in an accident and the owner is not present, it may not be as simple to allege negligence as in the traditional case where the owner is driving the car. However, one could allege negligence if the owner failed to maintain the autonomous car or failed to implement a software update. There may be questions regarding the conditions in which the AV features are turned on or off and the standard for when a vehicle occupant could or should override the autonomous driving system.

Liability questions for the manufacturer could include the accident avoidance algorithms and the automatic driving system, including how it chooses one accident avoidance maneuver over another when an accident is inevitable either way (should the AV have an accident with a large truck or pedestrians in an intersection?). Volvo and several other manufacturers have stated they

will accept liability for accidents involving their AVs, but this is with very few such vehicles on the road and no statistical resources or data regarding potential cost.

Product design considerations

Data is an increasingly valuable commodity and more products gather more information than ever before, through user input, environmental sensors, and network connectivity. A manufacturer must consider how it tracks processed data to ensure it can timely and efficiently retrieve data of a particular data subject if and when requested. Under the GDPR, data subjects have a right to request a copy of their data, to confirm whether their data is being processed, and to request their data be erased, or "forgotten." The GDPR requires that such data will be provided without cost, so any financial burden related to GDPR compliance must be accounted for in the development and pricing of new products.

A manufacturer must ensure customers are given the appropriate privacy notices required under the GDPR or other regulations which can vary depending on how their data is collected, such as directly from a customer, from a website where a potential customer seeks information, or from a third party. Applicable regulations must be considered, and compliance must be implemented through technical and organizational measures to protect data taking into account the state-of-the-art technology and cost of implementation. A basic approach is to include "privacy by design" to consider cyber security and privacy issues as a core tenet of product design and business practices.

The technology incorporated into smart products not only puts company or customer data at risk, sometimes the technology itself can be at risk. The United States Department of Transportation and Transport Canada announced in 2016 collaboration on communication between AVs and with transportation infrastructure technology to help ensure consistent development of the technology in both countries. However, many technologies used in smart products can also be used in weapons systems or otherwise raise national security issues. Consequently, such technologies may be subject to export controls of U.S. or Canada. The U.S. Export Administration Regulations control the export of dual-use products and technology from the U.S. as well as re-exportation from other countries.

The Export Control Reform Act of 2018 provides that the U.S. Department of Commerce establish controls for the export, re-export, and subsequent use of emerging technology. The U.S. Bureau of Industry and Security controls the export of items under the Export Administration Regulations and proposed rules in November 2018 regarding the criteria used to identify emerging technologies essential to U.S. security. It is likely that some of the components of artificial intelligence that help AVs safely navigate the roads would be considered critical technologies. How fast and how broadly smart technologies are adopted depends in large part on close collaboration among governmental bodies, industry organizations, and corporations creating new smart products. The closer the collaboration and more consistent the standards around the world, the faster and more ubiquitous smart technologies will become.

Vendor relations

Companies often rely on vendors to account for cyber security issues when they purchase products or services. However, it requires diligent vetting of the vendor to confirm all aspects of cyber security risk are accounted for, including local, state, national, and international regulations

as appropriate for the product or service. The terms of a vendor relationship can vary depending on the product or service at issues. A vendor providing financial services or software to enable control of an AV is more critical than less sensitive functions such as a motion sensor on a security light.

While certain regulations a company must follow may not apply to its vendors, it may be a good practice to require vendors who provide smart technology or connected products or services to maintain a similar level of cyber security standards, so the vendor's technology does not inadvertently become a backdoor that enables a breach through unauthorized access to the company's system or data.

Given the continually changing technology used in products, regulations regarding data security, and the abilities of wrongdoers to infiltrate technology systems, it is an ongoing standard to act "commercially reasonable" in providing security features for smart products. Different agencies have published cyber security guides, such as the Federal Trade Commission, Federal Communications Commission, and the Food and Drug Administration.

Companies can help ensure their vendors maintain appropriate cyber security standards as well by including contract terms that outline the specific safeguards that must be implemented under the applicable regulations, such as physical security, password management, and standards of training for the vendor's personnel. It is also important to require your vendors to have appropriate cyber security insurance in the event there is an incident that requires breach reporting to customers or responding to a governmental investigation. Companies must closely review the corporation's insurance program to make sure there are no gaps between its cyber security policy and the coverage provided by the vendor.

Where a third party is collecting or processing a company's data or the data of its customers, it is important to know how the vendor processes the data to ensure it complies with all applicable statutory regulations. If an American company has a vendor that uses a vendor that processes sensitive customer data in Europe or China, it may require significant additional analysis to confirm compliance with their laws, such as the GDPR or the China Internet Security law.

Designing the user into the product

Biometrics, the measurement of a person's physical characteristics, are becoming increasingly important to ensure secure access to smart devices. Biometrics, such as voice recognition, eye scans, fingerprints, and facial recognition can be used as security features to access devices, but biometrics are also personal information that can be used to identify and track people. A scan of your face can unlock an iPhone X and can be used to access financial accounts, but most people do not know where the data related to such a face scan is stored. There may come a time when such biometrics can be replicated.

Illinois implemented the Biometric Information Privacy Act in 2008 which was the first state law regulating the collection of biometric data. The statute requires informed consent prior to collection or disclosure of biometric data, outlines security and data retention guidelines, and creates a private cause of action for harms caused by violations. Texas and Washington have also passed statutes protecting biometric privacy, requiring consent before collecting biometric data, but there is no private cause of action as in Illinois.

Unlike a username or password, biometric data is generally permanent and not transferable from person to person. The uniqueness of biometric data can also be its shortcoming, because it

cannot be modified or replaced like a password and could be more difficult to repair in the event of a breach.

Conclusion

The new features available in smart products are endless and include conveniences not imagined twenty years ago. Smart products are only as "smart" as the data they collect but in doing so, manufacturers must stay up to date with the patchwork of cyber security and privacy laws across the world require. Cyber security is an evolving concept that requires not only digital security features, but also hardware protections, physical environment protections such as locked rooms and buildings, and human awareness and attention that must be continually updated over time.