2022 Product Liability & Complex Torts Seminar

June 1-3, 2022

RISE OF THE MACHINES:

Where is the Internet of Things today and where will it be tomorrow?

Bob deRosset
Moderator
YOUNG MOORE AND HENDERSON, P.A.
Raleigh, North Carolina
bob.derosset@youngmoorelaw.com

Christin Krämer
TIEFENBACHER
Heidelberg, Germany
kraemer@tiefenbacher.de

1. Growth of the industry and why it is important

The Internet of Things ("IoT") refers to physical products or equipment that can collect and share data and possibly other interactions such as remote control by the internet. The IoT is the melding of the physical and digital worlds. IoT devices communicate with each other as well as with people. The IoT is present in almost every industry. Named sectors of the IoT include the Industrial IoT (energy management systems, water distribution, factory automation, and vendor interaction), the Medical IoT (medical devices such as internal defibrillators, glucose monitors, and hospital systems including radiology and medication infusion pumps), and the Consumer IoT (smart watches, wireless keyboards, smart thermostats and lightbulbs).

IoT devices have limited processing and storage capability which can make it more difficult to implement security software such as anti-virus protection and may not be accessible remotely such that the manufacturer can monitor each product or update the software. Seemingly small vulnerabilities can have a big impact.

In the Industrial IoT, in June 2021, JBS Foods, one of the largest meat producers in the U.S. paid an $11 million ransom after an attack knocked out operations at its largest facilities in late May. This followed an attack on Colonial Pipeline, who was forced to shut down gas delivery to the East Coast and paid a $4.4 million ransom.

Despite the increased risk, IoT devices can be valuable. They can provide real-time collection and analysis of performance/functional information, increased agility, efficiency, collect input information, consumer information, environmental data, increase customer engagement, and countless other functions.

Most everyone encounters the IoT in their daily lives. They are present in the public infrastructure (sensors and cameras that collect and manage traffic data), in our personal lives (thermostats and light bulbs that you control from your phone), and our work (wireless keyboards, keycard door locks). It is critical that everyone, including consumers, government agencies, manufacturers and other companies involved with IoT technology, be engaged and situationally aware of cybersecurity issues. We all need to be cyber smart.

2. Current and proposed regulations (including obstacles to and gaps in regulation)

a. EU's General Data Protection Regulations (GDPR)

Under European law the protection of individuals with regard to the processing of personal data is a fundamental right. In accordance with art. 8 para. 1 of the Charter of Fundamental Rights of the European Union and art. 16 para. 1 of the Treaty on the Functioning of the European Union, everyone has the right to the protection of their personal data. The principles and rules under the GDPR relating to the protection of individuals with regard to the processing of their personal data should ensure that their fundamental rights and freedoms, and in particular their right to the protection of personal data, are respected, regardless of their nationality or place of residence.

In general, the GDPR applies to the processing of personal data insofar as it is carried out in the context of the activities of an establishment of a controller or processor in the European Union, regardless of whether the processing takes place in the Union. "Personal data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Additionally, "processing" means any operation or set of operations which is performed upon personal data, whether or not by automatic

means, such as collection, recording, organization, filing, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

As these definitions of personal data and processing are very wide, many IoT applications must comply with the GDPR. This may be very challenging, as the processor or controller is not only obliged to comply with certain processing rules but must also take organizational measures to protect personal data. Furthermore, any infringement can lead to massive damages under sec. 82 GDPR. Such claims for damages entail considerable risks for companies, because they often involve a large number of potential plaintiffs and are based on very similar or even identical facts.

Another very critical point is that if the controller or processor is transferring data outside the European Union, it must be ensured that the regulations of the GDPR are also complied with outside the European Union. Especially when transferring personal data to the United States, this may be very challenging as the United States is labeled as an "insecure" third country under the data protection policy. Also the Court of Justice of the European Union deemed the EU-US-Privacy-Shield as invalid. Therefore, companies must structure their contracts in such a way that they also guarantee the compliance with the GDPR in third countries. Just recently the Commission provided such safeguards by publishing such "standard data protection clauses." These clauses can be used to guarantee the safeguard of the GDPR in third countries.

Under the GDPR any infringement can lead to a penalty of up to 4% of a company's worldwide revenue from the preceding financial year or €20 million, whichever amount is higher, depending on the severity of the infringement.

IoT Highlights:

i. Personal data is generated more quickly than is often assumed. Nearly any data can be personal (e.g., just save data under a user account).

ii. One-off IT security measures are not enough in this respect. Rather, those responsible must consider further developments in information security and, if necessary, implement them.

iii. Identifying the data controller or processor is critical, and there are often more than one (e.g., for self-driving cars it may depend on the technology used – the owner, the driver or the manufacturer of the vehicle can be the controller or processor of the respective data).

b. European product liability laws

Under the Directive 85/374/EEC and the corresponding Act on Liability for Defective Products producers are liable if a defect in a product causes a person's death, injury to his body or damage to his health, or damage to an item of property. The producer of the product has an obligation to compensate the injured person for the resulting damage, sec, 1 para. 1 Act on Liability for Defective Products.

This legislation applies to any product marketed in the European Economic Area. Compensation for material damage is limited to goods for private use or consumption with a lower threshold of €500. It sets out a time limit of three years for the recovery of damages and forbids clauses limiting or excluding the liability of the producer. It is the injured party's responsibility to prove the damage, the defect and the causal relationship between defect and damage for the purpose of compensation.

Producers can be cleared of liability under certain conditions, notably, if they prove that:

i. they did not put the product into circulation;

ii. the defect was due to the compliance of the product with mandatory regulations issued by public authorities; or

iii. the state of scientific or technical knowledge at the time the product was put into circulation could not detect the defect.

The Directive and the Act on Liability for Defective Products only covers physical goods. Services do not fall into the scope of application. Software is considered a service, so an important legal gap, or at least uncertainty, exists between the physical side of an IoT device and its software. Therefore, the liability arising from the sale of any IoT product must be clearly determined in advance.

Nonetheless, manufacturers may be liable under national product liability law. Under German tort law a provider of software is liable as well. He is subject to a product monitoring and warning obligation. The product monitoring obligation requires the manufacturer to confirm whether its product is still safe even after it has been placed on the market. Furthermore, the manufacturer is obligated to warn of product hazards and to instruct the user accordingly.

IoT Highlights:

i. Even if the manufacturer of an IoT Product may not be liable under European law, he may be under national law.

ii. The manufacturer may be obligated to constantly update the corresponding software, depending on the product itself.

iii. The manufacturer is obligated to warn the customer about certain product errors.

c. Proposed measures from the Department for Culture, Media and Sport (DCMS) have been developed in conjunction with the UK's National Cyber Security Centre (NCSC), and would require that IoT devices sold in the UK must follow three rules:

i. all consumer internet-connected device passwords must be unique and not resettable to any universal factory setting;

ii. manufacturers of consumer IoT devices must provide a public point of contact so anyone can report a vulnerability and it will be acted on in a timely manner; and

iii. manufacturers of consumer IoT devices must explicitly state the minimum length of time that the device will receive security updates at the point of sale, either in store or online.

d. IoT Cybersecurity Improvement Act of 2020

The Internet of Things Cybersecurity Improvement Act of 2020 became law in December 2020 and requires the National Institute of Standards and Technology and the Office of Management and Budget to take specific steps to increase cybersecurity of IoT devices and set standards regarding the appropriate use and management of IoT devices owned or controlled by federal agencies or connected to systems under control by federal agencies and to insure that the OMB reviews agency security policies based on NIST Standards. NIST must review and revise the standards every five years and the OMB must update policies as applicable to be consistent with NIST revisions. Federal agencies are prohibited from procuring or using an IoT device if the agency determines that using the device prevents compliance with the standards, subject to waiver where necessary for national security, research purposes, or where the device is secured using alternative effective methods.

e. State Legislation

In the absence of a federal standard, all fifty states and the District of Columbia have passed laws requiring some form of notification following a breach of personal information. Throughout 2021, numerous state legislatures have considered and, in some cases, enacted legislation to modify existing data breach statutes. Notable state enactments include: (1) CT HB 5310, which modifies existing notification requirements by, among other provisions, shortening the number of days a business has to notify affected users; (2) TX HB 3746, which requires the state Attorney General ("AG") to publicly disclose breach notifications it receives; (3) UT HB 80, which establishes an affirmative defense for legal actions that arise from data breaches if the defendant has a cybersecurity program in place.

Other state legislative proposals that have not passed followed similar themes, including potential expansions of breach reporting requirements. IL SB 2353 and HB 3412 would require notification to the state AG and TN SB 1540 and MO SB 222 proposed to reduce their respective states' time period before which businesses must notify consumers. Certain legislatures, such as Illinois, Georgia, and Nevada, also considered measures that would establish liability protections/affirmative defenses for businesses that comply with designated security practices. The state legislatures discussed here adjourned without passing the cited bills.

California enacted the first IoT specific security law in the United States, effective on January 1, 2020, and it generally requires that all IoT devices sold in California be equipped with security features that are appropriate to the nature of the device and the data it collects. The security features must be able to protect the device and information on the device from various threats. Default passwords are illegal. Given most manufacturers want to distribute products in the California market, this may help encourage uniformity among products and help protect devices in other states as well.

f. Autonomous Vehicles

The United States is a proving ground for testing and deployment of automated vehicle ("AVs"), though a comprehensive federal framework for AV deployment and testing does not yet exist. Instead, the U.S. Department of Transportation has taken a series of actions with respect to AVs, Congress has considered various AV-focused legislation, and the majority of states have enacted laws expressly permitting the operation of AVs.

i. U.S. Department of Transportation

DOT's National Highway Traffic Safety Administration ("NHTSA") is expected to modernize existing Federal Motor Vehicle Safety Standards ("FMVSS") to adapt to AV technology and develop new FMVSS that pertain to AVs. While NHTSA considers updates to the FMVSS to better address emerging technologies like AVs, AV manufacturers can seek exemptions from inapplicable FMVSS. For instance, Nuro, an American robotics company based in Mountain View, California, has been granted an exemption from certain requirements under the FMVSS and this exemption allows Nuro to operate its fully occupantless AV.

NHTSA has also issued guidance for the AV industry to safely conduct limited testing on public roads. A key issue for suppliers is the ability to individually conduct testing of their own equipment on public roads separate from original equipment manufacturers ("OEM"), who benefit from a legacy rule that allows for a limited number of exempt vehicles to operate on public roads.

The recent rise in fatalities and crashes associated with advanced driver assistance systems ("ADAS") technology has led to NHTSA issuing an Standing General Order requiring, among other things, increased incident reporting of both ADAS-equipped vehicles and ADS-equipped vehicles. Reports made by entities subject to the Order will be made publicly available. AV operators conducting testing may also voluntarily notify NHTSA of ongoing testing into an accessible public database through NHTSA's AV TEST Initiative.

Parallel to the focus on ADS testing and deployment is an initiative to update NHTSA's New Car Assessment Program ("NCAP"), which will begin the process for developing minimum performance standards for ADAS. Separately, NHTSA is also revising its rulemaking on safety principles for ADS, which would request comment on certain elements of a potential framework for ADS. Both items were issued in early 2021 and were captured in a regulatory withdrawal at the beginning of the Biden Administration.

ii. Congress

Congress continues to pursue federal legislation to develop a federal framework for AVs, though Congress has not passed comprehensive AV legislation to date. This Congress has considered a federal ADS framework for deployment of ADS systems on public roads, though the number of vehicles would be limited, and the type of vehicle would be capped by gross vehicle weight. The likelihood of implementation of such a framework remains unclear.

The surface transportation reauthorization process has resulted in multiple pending

requirements with respect to ADAS policy. The Senate Commerce Committee passed the Surface Transportation Investment Act by a vote of 25-3 on June 16, 2021, which would:

- Require all passenger motor vehicles to be equipped with certain crash avoidance technologies such as automatic emergency braking ("AEB"), lane keep assist, and blind spot monitoring. The bill would also require that minimum performance standards be issued for such technology.
- Require the NHTSA to finalize an update to the NCAP and incorporate additional ADAS technologies into the NCAP. The provision also would require ADAS technologies to be evaluated for effectiveness in detecting vulnerable road users.
- Require driver monitoring technology to detect impaired drivers and prevent vehicle operation by impaired drivers.

iii. States

Currently, there is express authority for AVs to operate in 29 states, and additional states are considering, or have recently considered, legislation that would expressly permit AVs to operate in the state. With respect to existing state laws, some states only allow AVs to operate pursuant to specific testing or pilot programs, while other states permit commercial deployment of the technology. In addition, there are states that have executive orders or laws that either preempt localities' ability to prevent AVs from operating in the state or require state agencies or working groups to prepare studies related to AVs.

iv. Adoption/Deployment

Initial deployment of ADS technology can currently be found in last mile delivery/robot applications, commercial vehicles, ride-hailing, and public transportation systems.

g. Cybersecurity and Autonomous Vehicles

i. Implications for Emerging Technologies

Although cybersecurity is not an issue unique to AVs and connected vehicles, it has important implications for emerging vehicle technologies. Recent digitization of in-car systems combined with the growing internet connectivity of many new features has transformed cars into mobile computers that are able to collect and share large quantities of data. While innovative technologies are creating safer and more efficient vehicles, the complexity of these connected systems may also present heightened cybersecurity risks. For example, connected vehicle technologies include equipment, applications, systems, or other technologies that enable vehicle-to-vehicle ("V2V"), vehicle-to-infrastructure ("V2I"), and vehicle-to-everything ("V2X") communications in support of communications-based safety, mobility, and environmental approaches to transportation. With these systems, data drawn from

electronic control units and sensors connected to a vehicle's Controller Area Network bus ("CAN bus") is broadcast to nearby vehicles and infrastructure, allowing the vehicle to communicate with its surroundings. To ensure secure operation of this communication, the source of each message must be trustworthy, and the message must be protected from outside interference or modification.

ii. Federal Legislation:

On May 17, 2021, Rep. Ted Lieu (D-CA) introduced H.R. 3280, the Ending Forced Arbitration for Victims of Data Breaches Act of 2021 ("bill"). The bill would ban mandatory arbitration for data breaches. Following introduction, the bill was referred to the House Committee on Energy and Commerce.

iii. Congressional Hearing Highlights:

During a wide range of congressional hearings throughout the 117th Congress, the future of data breach reporting requirements was discussed. During a House Committee on Financial Services' ("House Financial Services") Task Force on Artificial Intelligence ("AI Task Force") hearing on digital identity, Rep. Ted Budd (R-NC) expressed concern about a patchwork of data breach notification laws and an absence of a federal framework.

During the Senate Committee on Commerce, Science, and Transportation ("Senate Commerce") nomination hearing for Federal Trade Commission ("FTC") Chair Lina Khan, Chair Khan noted that data breaches pose a national security risk and outlined the FTC's small business education programs on data security practices.

Following the SolarWinds breach, the House Committee on Oversight and Reform ("House Oversight") and House Committee on Homeland Security ("House Homeland Security") convened a joint hearing to discuss the aftermath of the breach. Rep. Yvette Clarke (D-NY) expressed support for data breach legislation that would require companies to report such breaches to a federal agency. Rep. Kathleen Rice (D-NY) added that anonymity in breach reports could aid with private sector information sharing. Rep. Cori Bush (D-M) emphasized a need for data breach notification legislation.

The Senate Select Committee on Intelligence ("Senate Intelligence") held a similar hearing where Sen. John Cornyn (R-TX) expressed support for mandatory data breach notification requirements with liability protections for companies. Sen. Angus King (I-ME) expressed agreement that such requirements "may be necessary." Sen. Ben Sasse (R-NE) noted that there should be central agency for data breach notification. Sen. Mark Warner (D-VA) expressed support for a mandatory data breach reporting requirement.

iv. Congress is expected to vote on three main legislative packages this year. 1) Infrastructure (August 21); 2) Social Infrastructure (American Jobs and Families Plan, Labor Reform, Tax Reform, etc.)(by October 1); and 3) US Innovation and Competition Act (China competition)(by December 21).

Current Infrastructure package, as is, will both directly and indirectly impact AVs:

- Direct and Indirect:

    - Direct: Includes safety provisions that require adoption of more ADAS crash avoidance technology as standard on vehicles (*i.e.*, lane keep assist, AEB, Blind-Spot Detection, Lane Departure, adaptive cruise control etc.). These ADAS technologies are the building blocks of SAE levels of automated driving and will strengthen SAE Level 2 to start transition into higher levels.

    - Indirect: The increased focus and funding on improving highway infrastructure (roads and signage) will positively impact ADAS systems and improve performance (*i.e.*, land markings, high off ramp line markings, improved road side infrastructure).

  As is, the package also includes cybersecurity funding to develop more programs and provisions focusing on national grid systems in the energy sector, which the construct will be used as a model for connected transportation municipalities for transportation connectivity.

  Social Infrastructure package - Scope TBD - Will have provision that includes investments and credits for domestic R&D of technology across various sectors. Automotive industry is expected to see a benefit in spending, workforce development, and incentives to do more in the US.

  US Innovation and Competition Act - Primarily focused on Competition with China, will be expansive and have the biggest impact on both cybersecurity, data security, AVs, and Transportation Sector in general.

- AV bill, or a version of it, is anticipated to be pursued in this package.

- Export Controls on emerging and foundational technologies are anticipated to be expanded in this package, which will target AI, telecommunications, and other advanced technology components that will be adopted into the automotive industry. Semiconductors will be a driver in this. This package will expand export regime authority (CFIUS) that will subsequently impose domestic or certified purchasing requirements, and slowly impose purchase restrictions from non-allied nations on defined technologies/components to protect both US investment and national security.

- This includes updates to DHS CISA Critical Infrastructure and Industries to expand classifications and include new industries (*i.e.*, Automotive); subsequently will impose new compliance requirements for certain components and technologies we are developing in vehicles and infrastructure (*i.e.*, V2I).

- Data security will also be a focus in this package with regard to pushing for a federal framework instead of the patchwork of state data breach notification laws. Like other industries, the automotive industry has an ISAC that is going to handle mitigation of threats within the industry, and would be strengthened by provisions in the package.

v. Relevant Guidance

The NHTSA and other bodies such as the National Institute of Standards and Technology ("NIST"), the International Organization for Standardization ("ISO"), and SAE International have issued guidance to address cybersecurity challenges associated with connected vehicles, although manufacturers may also address cybersecurity in other, unique ways. Earlier this year, the NHTSA proposed updates to guidance on Cybersecurity Best Practices for the Safety of Modern Vehicles, while the Federal Trade Commission's ("FTC") mandate to protect consumer privacy has placed cybersecurity in connected vehicles squarely within the agency's regulatory reach. With increased connectivity in vehicles and potentially overlapping regulatory authority, stakeholders and consumer advocates alike are calling for the development of a uniform cybersecurity framework for AVs.

vi. UN Regulations on Cybersecurity and Software Updates, effective Jan. 2021

As the technological development and digitalization of in-vehicle systems progresses, automobiles become more and more connected. Cars offer much more than mobility. They have many more features, such as infotainment systems, that make a journey more pleasant. These features frequently require a connection to a remote server, which makes cybersecurity a top priority not only for the car maker but also for the occupants of the vehicle. If a hacker can gain control of the vehicle itself, it may cause disastrous, maybe deadly results.

The UN has issued two new regulations on Cybersecurity and Software Updates to provide a unified standard on tackling these risks. These regulations establish audit requirements and clear performance standards for car manufacturers.

The regulations apply to passenger cars, vans, trucks and buses a provide guidance for the following disciplines:

a) managing vehicle cyber risk;

b) securing vehicles by design to mitigate risks along the value chain;

c) detecting and responding to security incidents across vehicle fleet; and

d) providing safe and secure software updates and ensuring vehicle safety is not compromised, introducing a legal basis for so-called "Over-the-Air" (O.T.A.) updates to on-board vehicle software.

The UN Regulation on Cybersecurity and Cyber Security Management Systems provides a framework for the automotive sector to put in place the necessary processes to:

a) identify and manage cyber security risks in vehicle design;

b) verify that the risks are managed, including testing;

c) ensure that risk assessments are kept current;

d) monitor cyberattacks and effectively respond to them;

e) support analysis of successful or attempted attacks; and

f) assess if cyber security measures remain effective in light of new threats and vulnerabilities.

The UN Regulation on Software Updates and Software Updates Management Systems provides a framework for the automotive sector to implement processes for:

a) recording the hardware and software versions relevant to a vehicle type;

b) identifying software relevant for type approval;

c) verifying that the software on a component is what it should be;

d) identifying interdependencies, especially with regards to software updates;

e) identifying vehicle targets and verifying their compatibility with an update;

f) assessing whether a software update affects the type of approval or legally defined parameters (including adding or removing a function);

g) assessing if an update affects safety or safe driving;

h) informing vehicle owners of updates; and

i) documenting all the above.

Furthermore, the UN provides a list of vulnerability or attack methods related to the threats. This can help any car manufacturer assess potential risk factors and develop appropriate defense strategies and mechanisms.

3. Risks and liabilities

a. Security and privacy issues

A company can prepare for such attacks on its systems or its products by regularly evaluating the risks to their products and systems and ensuring there is a plan in place that has been tested for problems that inevitably arise. With an appropriate plan that has been tested, a company can put its plan into action and regenerate its systems or update its product and avoid loss of data or business interruption without paying a large ransom. A recent study found that 80% of the companies that paid ransom have been targeted again.

b. What law applies

Although about half the states in the U.S. have enacted data privacy laws, there is no comprehensive cybersecurity statute or privacy statute in the U.S. The wireless connections that hold the IoT together convey signals to and from products and people and many times the connectivity provider may be considered a telecommunications provider that is subject to existing regulations, such as licensing requirements, regulatory fees and penalties for

noncompliance.

The FDA issued a guidance document, *Policy for Device Software Functions and Mobile Medical Applications, Guidance for Industry and Food and Drug Administration Staff* in 2019 that focuses on whether a software function qualifies as a medical device as defined in the Food, Drug and Cosmetic Act. If the software function qualifies as a medical device, FDA regulations will apply, such as requiring pre-market clearance. Regulated medical devices include software that connects to a medical device to control the device or analyze data, performing patient specific analysis for diagnostic information, or where it is attached to sensors, attachments, or screens and the device includes functionality similar to other regulated devices. The Internet of Medical Things must be secure and be subject to higher scrutiny due to state and federal privacy laws for medical information. Connected medical devices must address data security plus privacy. This is particularly difficult when interoperability is critical for smart medical devices to access and exchange information that is reviewed and accessed by patients and a variety of healthcare providers.

In the EU eHealth sector, manufacturers of connected medical devices are subject to the EU Medical Device Regulations, effective May 2020, whereas connected medical device framework in the U.S. is voluntary under the FDA's guidelines. The U.S. may want to take steps to implement regulations consistent with other parts of the world, to encourage trade and product sales to other countries.

Manufacturers must also be aware of data localization rules where their smart products are sold or used. Data localization rules may require data concerning citizens of a jurisdiction to be stored, collected and processed within the jurisdiction of the citizen or where the data was collected. Harmonizing data security and IoT design standards across the globe should be a goal considering the market for IoT devices is global and protecting customer's information is simply good business.

c. Geopolitical, industrial, and consumer impact

From a legal perspective, IoT products are very challenging. The amount of risk that must be addressed by a company depends on its position in the IoT ecosystem. Companies that collect, process, and store data may have substantially greater risk than companies that simply facilitate transmission of data. Many smart products are highly innovative and provide services not seen before. As the law is regularly a summary of experiences from the past, the legal classification and the legal situation in general is unclear. In a globalized world, every smart product must be evaluated in the context of the differing laws wherever the product may be purchased, used, or accessed.

Cybersecurity may be a particularly challenging matter for smaller companies with a more limited product line. A small incident may have a huge impact on the company´s balance sheet. Especially if sensitive data is affected, the negative impact for a small company with only a small client base may be heavily affected. A proper cybersecurity strategy and insurance may be very costly. Small companies must therefore protect their intellectual property at relative high cost compared to large companies, which often have diversified products and services.

Whether a company or its customer base is large or small, a data breach or security breach of an IoT product can significantly impact a large number of people, both users and third parties. A very

popular IoT product may expose numerous users, but an IoT product with few users may expose even more third party information due to the nature of the product, such as an application that other companies use in their products to save user information.

A ransomware attack by a Russian crime organization on July 3, 2021 targeted Kaysea, a supply chain IT management software provide. The attack pushed a malicious update to Kaysea's clients and affected at least forty clients. Some of the clients were managed service providers that each work with hundreds of businesses, which significantly leverages the possible impact and damages. Just one example involved a Swedish grocery store chain that was forced to close more than 800 stores because their systems were down. The criminals demanded ransoms such as $50,000 per employee, but this is in addition to the impact on the company's reputation with its customers and possible regulatory penalties.

If a company is attacked by a hacker or a group of hackers, the pursuit of damages may be impossible. The hacker may live in another country. Furthermore, many states are involved in hacking other countries companies to gain an advantage. Since these hackers are regularly financed by a state, they may be in a better financial position than many attacked companies.

If a manufacturer wants to sell its products in many different countries, it must comply with laws that often differ across jurisdictions. In a globalized world, where many services are offered on the internet and the seller may not even intend to sell his services to a certain country, it may be very challenging to comply with the regarding laws. In this case, large companies have an advantage over small companies. Violations are often heavily penalized, so any product or service offering to other countries must be properly assessed for compliance with all applicable regulations.

Finally, as stated above, GDPR-infringements may be punishable with fines of up to up to 4% of a company's worldwide revenue from the preceding financial year or €20 million, whichever amount is higher (e.g., the Swedish retailer H&M was fined €35.3 million in 2020). In recent years, fines have trended upward. Small companies are hit much harder by this than large companies, which are better able to absorb such financial burdens.

d. Evolving standards

Litigation involving IoT products may include a wider variety of defendants, such as the manufacturer, the company that facilitated data transmission, a cloud storage provider, etc. Expert evidence in such a lawsuit is more complex. While an engineer may be able to offer testimony about functionality of a smart product, a programmer may be necessary to address software issues. Artificial intelligence adds a significant layer of complexity. As smart devices with AI increasingly have the ability to collect information and build on that information, learning and making decisions based on the data, a point will come when artificial intelligence decision-making may surpass human ability. In certain instances there may be a time when a product's AI surpasses a human expert's opinion and a question may arise whether there could be a product malfunction or the human programmer who created the artificial intelligence could be responsible. Products with AI collect large amounts of data over time and make decisions in ways that are different from when the product was new.

Industrial IoT products often include sensors in manufacturing processes that help predict when a component may fail so it can be replaced before causing damage or company downtime. Such

information can improve supply chain management and just in time delivery of materials and production management, but may expose a company to potential liability before a failure has even occurred.

4. Best practices for manufacturers

a. Be proactive in meeting regulatory standards

Being proactive in meeting regulatory standards brings many benefits. First, many customers will appreciate a high level of safety. Second, a company can avoid hefty fines, image loss and damage to the brand. Third, proactive management of legal standards may create the opportunity to create a new standard itself.

From a legal perspective there are many unresolved issues regard IoT products. These products are still too new for the legislature to have fully regulated them. In addition, these products are evolving at a very fast pace, so it is to be expected that the regulators will continue to lag behind this evolution. Companies may create new technology which may become the future regulatory standard. This creates the unique opportunity to gain an advantage by self-regulating your own products. If this regulation proves to be practical it may become the legal standard, creating a significant competitive advantage.

Furthermore, as there are many unresolved issues, smart management of authority requests can avoid a lot of trouble. A cooperative relationship with the regulatory authority can help to create trust in the self-regulatory status of the company. Additionally, it can help avoid unexpected regulation which may require product changes.

b. Security as a competitive advantage

Cybersecurity and data protection can be a competitive advantage as well. In contrast to Facebook, Apple products have shown security as an advantage. While there have been many discussions about Facebook regarding privacy laws, the same discussions did not arise around Apple´s products. Especially in Europe, where data protection is a very sensitive issue, companies need to handle these topics with particular care.

An effective data protection policy must be drafted with precision to avoid any unintended effects. As the fines and the potential loss of customers by any infringement of the GDPR are likely to be very high, data protection management must be taken very seriously. A good data protection policy not only includes standard procedures for handling personal data but also includes organizational matters to assure the policy is applied correctly, a step-by-step explanation on how to deal with infringement and data breach, and periodic assessment of whether policies need to be adjusted.

One way to help develop information security as a marketable product feature is to increase awareness and customer education on these issues and more transparency regarding data collection, processing, and storage. Manufacturers must consider that security in their connected products is a significant feature and competitive advantage. Instead of data security and regulatory compliance being an afterthought, it can be a significant motivating factor when a customer makes a purchasing decision.

c. Security by design

Security by design is a development practice that reduces cyber risk by using a disciplined process of continuous testing, authentication safeguards and adherence to best development practices. Security by design principles "embed security in the technology and system development from the early stages of conceptualization and design." Security standards should be used to guide the development process. FCC White Paper, Cybersecurity Risk Reduction, January 18, 2017.

d. Secure Internet Protocols, Cyber Hygiene, Strong Authentication, Cyber Education

Digital security is easy to overlook, you cannot see it or touch it, but it is important that we learn to consider it as a real tangible thing. Our parking garages often have gates that require keycard access, our office buildings have locked doors and security guards, the digital security of your company's systems and products must be considered just as important. Digital attacks such as ransomware are a threat to a company's core business operations and it is critical to integrate security into your company's DNA for both internal operations and product development. In June 2021, President Biden signed an Executive Order, *Improving the Nation's Cybersecurity*, which includes several general best practices that are concrete steps to take that help protect companies and their products. Some of these best practices include:

i. Multi-factor authentication (such as when logging in you enter your username and password and the system sends you a one-time code by email or text message that you have to enter within a brief time to finish logging in) is helpful because even if your password is compromised, a criminal still cannot log into your account.

ii. Endpoint detection and response capability that identifies malicious activity on a network is important, because without this ability a criminal can access a system and you will not know it is there until it takes additional action.

iii. Data encryption is important so that if data is stolen it still cannot be read or used.

iv. Dedicated personnel who stay up-to-date with changes in technology, regulations, and best practices are better prepared to identify threats, correct problems and strengthen weak points on an ongoing basis.

v. Back up your data, keep the backups offline, and regularly test them. With adequate backup data, if a company experiences a ransomware attack, its system can be restored and continue operating, with very little downtime and without paying a ransom.

vi. Update and patch systems consistently and timely.

vii. Test your incident response plan. Many weaknesses in a data security plan may not become apparent until you actually try to use it. For example, if a company experienced a breach in its accounting system, consider whether manufacturing operations continue or would they have to be shut down as well.

viii. Have a third-party test your systems and security plan. This is confirmation that your inhouse people have not overlooked something.

ix. Segment your networks. Cybersecurity attacks may involve ransomware and a demand for money, but may also involve data theft or simply disrupting operations. Business

functions and manufacturing or production operations that are separated can help insure that compromise of one side does not mean all sections of the company are involved. Separate parts of the network can be linked strategically or with manual controls to help insure that critical functions can be maintained during any incident.

e. Product design considerations for an evolving future; how a standard regulatory framework could reduce product development costs and liability exposure

Manufacturers must plan for obsolescence of smart devices from the beginning. While regulating the design and technology standards for new products may help protect customers, it is more effective to address such risk at the network level where digital security solutions can benefit people and products in a more comprehensive manner than standards for individual products.

The FCC has focused on monitoring and regulating internet security at the network level, which should have a positive trickle-down effect on security to individual products. The FCC and many other governmental agencies and professional organizations encourage "security by design." Given the diverse industries and functions of companies that impact the IoT, security by design is a flexible concept that must be adapted for the intended use.

The FCC issued a white paper on cybersecurity risk reduction in January 2017, noting that the Department of Homeland Security had issued principals regarding IoT security that called on the public and private sectors to work together to improve IoT security. The attack surface created by the IoT is growing exponentially and there is a widening gap between the ideal investment in cybersecurity between the commercial point of view and the consumer's view. This gap will likely expand as the IoT becomes more prevalent in certain sectors such as public safety communication, industrial control systems, and smart city technologies.

From a company's perspective, it will continue investing in cybersecurity as long as the expected benefit exceeds the cost, but at some point the marginal benefit decreases until additional investment is unlikely. There is always residual risk that remains and companies accept the risk. When residual risk remains in a marketplace, third parties step in to respond to the risk and they may create alternative solutions for the risk. If the residual risk is relatively significant, companies may purchase insurance to account for the remaining risk. Insurers increasingly require accountability for cybersecurity issues when placing coverage. Governments, consumers, or industry groups may help mitigate residual risk through increased investments, industry standards, political pressure, or regulation. Lastly, residual risk can be transferred to third parties such as the internet service providers.

While coordinated top down standards and regulations are important for purposes of market stability and interoperability, it is still important that companies and their customers understand the risks that IoT devices may present and how the risk is modified when the product is integrated into their own larger network of systems and devices.

One way to help develop information security as a marketable product feature is to increase awareness and customer education on these issues and more transparency regarding data collection, processing, and storage.