Recent IoT Class Actions Highlight Need for Manufacturers & Vendors of Connected Products to Be Aware of Liability Risks

The Internet of Things (IoT) products have become a way of life. There are huge benefits of "smart" products, which interact through the internet to gather and exchange data to provide additional functions, security, and easy use for consumers. These "smart" products are present in our everyday lives, including such standard products as refrigerators, watches, fire alarms, door locks, security systems, and fitness trackers. These are only a few examples of the many IoT products on the market today. However, in spite of the significant benefits provided by connected products, the new technology raises thorny legal issues and is leading to litigation.

In the last several weeks, two cases have been filed in California against Amazon related to its Ring security devices.

The first case, filed on December 26, 2019, alleges that children were playing basketball at their Alabama home when a hacker spoke to the kids thought the Ring device installed on the garage. The hacker spoke to the kids, commenting on their basketball skills and asking them to get closer to the camera. The lawsuit filed by the children's father alleges common law negligence and invasion of privacy, seeking $5 million in damages as well as declaratory and injunctive relief.

The second lawsuit is a class action filed on January 3, 2020. Plaintiffs in this lawsuit allege that the security devices and systems are defective because they contain vulnerabilities that allow hackers to spy on and harass consumers where they live. The complaint describes how hackers used Ring security devices to scare and taunt families in both Mississippi and Texas. In Mississippi, a hacker used a Ring device to call an 8-year-old girl racial slurs, play songs from horror movies and encourage the girl to misbehave. In Texas, the hacker spoke to the family through the indoor Ring camera and said, "I'm outside your door," and threatened the family with "termination" if they did not pay a ransom. Plaintiffs are alleging negligence, breach of implied contract, intrusion upon seclusion and public disclosure of facts. While such class action lawsuits may not get far until a class is certified; even after certification, the class may not succeed unless they can show specific harm related to the alleged breach.

While these cases have focused on product failures and torts, a myriad of data privacy laws may also be implicated. For example, under California's new Consumer Protection Act, any personal information a company has about a consumer (i.e., individual) has to be protected using appropriate technical and administrative safeguards. If an IoT device allows an unauthorized third party to access or see "personal information," which has a broad definition that can include an IP address, then the provider of that device could be subject to a data privacy claim. In addition, some states have laws protecting biometric data, which includes facial scans, etc., that could be implicated in IoT devices using video technology.

Hacks similar to those in the Ring, LLC cases have been reported across the country. Given the exposure documented in the Ring cases and the lack of consensus surrounding the standards and legal frameworks that govern design, manufacture, and performance of IoT products in general, companies are left without much direction for avoiding litigation. However, we've seen areas in which manufacturers are at higher risk for litigation within existing laws. We've outlined a few of those risk areas below.

- **Hard-coded passwords, hacking, and privacy.** Some smart home devices come with hard-coded passwords (these passwords are often easily available on the web) that outsiders with malicious intentions could access to remotely break in and steal user data,

access facial images or other personal information. Horror stories of privacy invasion, including examples of hackers tapping into home baby monitors or the recording of conversations via smart speakers, are, unfortunately, not uncommon. The liability potential for privacy issues may include notice obligations, reporting to regulatory agencies, regulatory fines and penalties, individual claims and liabilities and, of course, the possibility of class claims.

- **Failures of connected devices leading to injury or property damage.** If a connected product uses a "cyber-physical system" of software and networking to control real-world physical objects—such as home appliances and machines—and if the product fails, this failure could cause bodily or personal property damage. For example, if a smart thermostat in a water heater is programmed to turn off at a certain temperature but a software failure prevents it from activating, water temperature levels could become dangerously hot and consumers could be burned.

- **More complex liability standard**. Some states recognize the "consumer expectation" test, which requires that additional questions apply to design defect allegations. When a consumer purchases a connected product, does the consumer expect that hackers will be able to infiltrate the software? Does the consumer expect that the product will be designed in a manner in which the software can malfunction if

the software is not updated in a timely manner, or if the software update is interrupted? If answered in the negative, the manufacturer may be subject to liability. This public policy related claim is also potentially a trigger for a class claim.

- **Lack of insurance coverage.** Connected products and hacking may also raise insurance coverage issues. If the hacker activities are deemed "terrorism," or if the appropriate steps to preclude such hacker access were negligently or intentionally not incorporated into the IoT device, insurance coverage in a standard policy may be excluded or significantly limited. All connected-products stakeholders (manufacturers, importers, software designers, app developers, etc.) must evaluate their insurance coverage and may need to purchase additional insurance coverage specifically designed for their business and the potential risks. Most commercial general liability coverage (for property damage and personal injury) expressly exclude technology. Cyber liability policies (e.g., data breach coverage, network intrusion coverage, etc.) are additional policies that should be considered to ensure that the product's liability possibilities are fully covered.

- **CPSC regulation.** The Consumer Product Safety Commission has been pressed recently to adopt stricter regulations for connected products. If the Commission decides to promulgate stronger

regulations, the risk of a recall could potentially create greater liability for manufacturers.

- **Assigning liability.** Traditional products liability principles apply reasonably well to connected devices when the device itself malfunctions. For example, liability for burst pipes due to a smart thermostat's failure to activate can be analyzed and allocated under traditional design or manufacturing defect concepts. The potential for a malfunction due to a software failure, however, adds a layer of complexity to the analysis, including determination of whether the software was defective and allocation of liability for any defect between the device manufacturer and the software supplier. New categories of computer experts are often required to pursue or defend such claims. Liability is significantly more difficult to judge in the connected products realm, where devices are increasingly integrated into networks. In addition, if the product manufacturer contracts for the software component or the data hosting component, which leads to the potential liability, there may be contract considerations as to the ability to shift liability downstream to the licensor or the data host provider.

- **Increased damages risks.** The types of damages resulting from data security breaches typically are not recoverable under existing products liability law (see the note above on cyber liability insurance). In most instances, products liability law permits recovery of

damages arising from personal injury or physical damage to property, but bars recovery for purely economic losses, including business disruption and other purely financial losses. It is unlikely that this traditional shield from economic damages will hold up when a device manufacturer's software defect allows a hacker to engage in mass financial fraud or identity theft, or creates massive business interruptions from a disabled network. The increasing number of new data privacy regulations and regulatory compliance protocols require new actions to mitigate or avoid additional penalties.

For manufacturers of IoT products, the following best practices can help minimize the risk of litigation:

- Audit existing policies, which are necessary to ensure that data privacy, data breach and regulatory notice obligations are documented.

- Create and follow checklists for immediately investigating and mitigating risks that should be followed upon notice of an issue that implicates problems beyond product failure (i.e., data breach, failure to comply with applicable law, etc.).

- Verify that personnel training includes obligations to protect and respond to any data or other regulatory requirements.

- Ensure that contracts with licensors and third-party service providers (such as data host providers) address any shifting of liability, limits on liability and notice obligations, all consistent with applicable laws.

- Audit jurisdictions applicable to the IoT devices to ensure that a full awareness of the possible implicated laws and regulations has been assessed to ensure compliance.

- Comply with industry standards, such as the National Institute of Science and Technology's NIST Special Publication 800-66 Rev 1 on "Information Security," NIST Special Publication 800-88 Rev 1 on "Guidelines for Media Sanitization," and NIST Special Publication 800-61 Rev 2 on "Computer Security Incident Handling Guide."