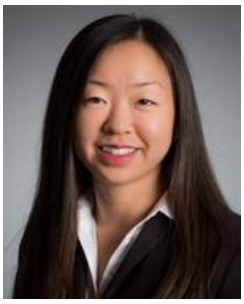
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Connected Devices Bring New Product Liability Challenges

By **Erin Bosman, Julie Park and Benjamin Kagel**
January 5, 2018, 11:28 AM EST

Erin Bosman



Julie Park

Benjamin Kagel

"My Google Home Mini was inadvertently spying on me 24/7 due to a hardware flaw," wrote a tech blogger who purchased Google Inc.'s latest internet of things (IoT) device. Following the incident, a pact of consumer advocacy groups insisted the U.S. Consumer Product Safety Commission recall the Google smart speaker due to privacy concerns arising when the device recorded all audio without voice command prompts.

The CPSC is charged with protecting consumers from products that pose potential hazards. Traditionally, this has meant hazards that may cause physical injury or property damage. But as internet-connected household products continue to proliferate, issues like the "always-on" Google Home Mini raise an important question: Where does cybersecurity of consumer IoT devices fit within the current legal framework governing consumer products?

The Explosion of IoT

Forecasts predict that by 2020 IoT devices will account for 24 billion of the 34 billion devices connected to the internet. According to a recent Gemalto survey, "[a] hacker controlling IoT devices is the most common concern for consumers (65 percent), while six in ten (60 percent) worry about their data being stolen."

The rapid growth of the IoT market and continued integration into daily life raises the question of which regulatory body or bodies, if any, should be responsible for consumer safety when it comes to cybersecurity for consumer IoT devices.

The Intersection of Consumer Product Safety, Privacy and Cybersecurity

The CPSC's jurisdiction has traditionally been limited to physical injury and property damage. It is "charged with protecting the public from unreasonable risks of injury or death associated with the use of the thousands of types of consumer products under the agency's jurisdiction."

Companies reporting potential safety hazards are given the option to categorize the hazard as fire,

mechanical, electrocution, chemical or "other." But "other" has never been used to describe a hazard that did not involve a personal injury or property damage risk. CPSC enforcement actions against manufacturers of IoT devices for security defects that do not lead to physical injury or property damage would be unprecedented.

One way to think about CPSC's potential jurisdiction is over incidents that could give rise to product liability claims. Product liability primarily aims to compensate consumers and bystanders for injuries caused by unsafe products and to incentivize manufacturers and supply-chain participants to take reasonable precautions in producing and distributing products. The underlying policy rationale is that manufacturers are typically in the best position to prevent harms caused by their products.

Product recalls seek to remove unsafe products from the market and prevent product liability claims from arising in the first place. But when does a privacy or security breach reach the threshold of a safety hazard or a product defect such that it mandates a recall? And what role do product recalls even play in an age where companies can deploy firmware updates to implement a corrective action for privacy or security breaches?

The very features that are potential weaknesses for IoT devices can also be leveraged as strengths. Google demonstrated this by issuing a security patch to address the "always-on" issue in its Google Home Mini.

Protecting Your Business in the Face of Regulatory Uncertainty

How do IoT companies manage regulatory compliance where the regulatory framework is so uncertain and regulators are unable to keep up with technological developments? One possible construct is to anticipate traditional product defect claims that consumers might bring against IoT products, and use the power of connected devices to safeguard against liability while also protecting the product brand.

Take, for example, manufacturing defects. Courts may find that errors or oversights in coding, random malfunctions or bugs in the system constitute product liability claims for manufacturing or design defects. But IoT companies can also look at ways to put checks in place to catch these issues early. And the ability of connected devices to provide effective — and even fun — warnings and instructions to consumers about possible flaws is limited only by developers' creativity.

What about failure to warn? Product manufacturers have traditionally had a duty to warn of risks that they know about or reasonably should have known about. We recently wrote about the growing role of artificial intelligence and the implications of product manufacturers' ability to mine big data. Companies that choose to collect and store that data do assume risks, but they also have the ability to assess problems and develop innovative ways to provide warnings about them.

It will take years for government regulators to catch up to these issues and enact applicable regulations, particularly in light of the current administration's trend toward deregulation. This is a golden opportunity for IoT manufacturers to create their own framework for how best to protect consumers and to balance the risks and benefits of IoT devices.

Where Do New Risks Fit into the Old Framework?

Undoubtedly, the existing product liability framework has limits and doesn't map perfectly to IoT devices. Consider the "always-on" feature recently brought to the CPSC's attention. Under the economic

loss doctrine, a plaintiff cannot recover monetary damages that don't arise from physical injury to her person or physical harm to her property. Security breaches may cause an invasion of privacy without causing any physical injury, making the product liability framework inapplicable.

As shown by the recent consumer advocacy letter, these groups may argue that security considerations and subsequent risks of IoT devices — while different from traditional public safety concerns — still fall within the CPSC's broad mandate to "protect the public against unreasonable risk of injuries and death associated with consumer products." But without a clear CPSC directive that an injury to privacy falls within the requirements to report a safety hazard, IoT manufacturers would be voluntarily involving CPSC should they decide to report incidents similar to the Google Home Mini.

Although new regulations could fill the cybersecurity gap, technological innovation is far outpacing regulatory agencies. By the time applicable regulations are in place, they may already be out of date. Consequently, it is incumbent upon industry leaders to work together to pave the way for a robust cybersecurity framework that avoids stifling innovation by overregulation while still protecting consumers from security vulnerabilities.

Advances in IoT technology and its continued integration into everyday life are changing traditional notions of consumer product safety. Working closely with product liability, privacy and cybersecurity specialists will allow IoT companies to anticipate legal issues and use technology to stay ahead of regulatory enforcement and consumer-driven lawsuits.

Erin M. Bosman and Julie Y. Park are partners and Benjamin S. Kagel is an associate at Morrison & Foerster LLP in San Diego.