THE
NATIONAL LAW REVIEW

CPSC Commissioner Elliot Kaye Issues Statement Providing a Framework of Safety for the Internet of Things

Monday, February 11, 2019

In recent years, the U.S. Consumer Product Safety Commission (CPSC) has begun to grapple with the effects of the Internet of Things (IoT) on consumer product safety. In May 2018, the CPSC held its first public hearing regarding IoT devices, during which the agency sought to jump-start a conversation on the appropriate framework for consumer product safety practices and IoT devices. In an effort to carry on this conversation, Commissioner Elliot Kaye recently released a framework, which he co-authored with his Senior Science and Policy Advisor, Dr. Jonathan Midgett, that provides an "overview of technology-neutral best practices to ensure consumer product safety in the design and deployment of devices, software, and systems used with the Internet-connected consumer products." This framework should prove useful to consumer product companies as they navigate the burgeoning world of IoT devices.

Article By Matthew R. Howsare Charles A. SamuelsEvelyn FrenchMintz Alert!

Consumer Protection
Products Liability
Communications, Media & Internet
Administrative & Regulatory
All Federal

For those readers unfamiliar with the topic, IoT is typically defined as a group of devices that have internet connectivity which enables them to communicate and interact with each other and collect data. In recent years, the number of IoT devices has expanded exponentially to include everyday devices such as home appliances, fitness wearables, and children's toys. While these devices have many tangible benefits to consumers, they present their own set of risks to product safety. For example, what if a software update to a connected product goes awry, causing the product to overheat? Or what if malware infects a connected product, causing the product to malfunction? Indeed, the CPSC has already addressed an IoT device defect when the IoT-connected Nest Protect Smoke + CO alarm was recalled in 2014 for having a feature that allowed the user to temporarily but unintentionally silence some alerts or cancel a manual test by vigorously waving an arm near the device.

In an effort to address these new potential risks, Commissioner Kaye and Dr. Midgett published the above-mentioned framework. This framework is not intended to address issues related to personal privacy or data confidentiality, as those topics are the focus of other regulatory agencies such as the Federal Trade Commission and the Federal Communications Commission. Instead, the framework is focused exclusively on consumer product safety.

The framework begins by highlighting the roles and responsibilities of manufacturers and retailers of IoT devices. Both manufacturers and retailers "should anticipate safety concerns as new capabilities are added to the IoT ecosystem" and should have in place safety guidance procedures for both the product development phase and the lifespan of the product. Additionally, the framework recommends that a qualified safety supervisor "be assigned to monitor the development and marketing of each product and product component of an IoT system, including the safety of the software upon which the product relies for functionality." Such a suggestion is

considered a good practice of a robust product safety compliance program, irrespective of IoT devices.

Next, the framework addresses the necessary risk assessment that manufacturers should employ when developing connected devices. Importantly, it states that this risk assessment should be conducted for every product function, software update, and stage of the product's lifecycle. Among other considerations, this risk assessment should consider:

- The intended end user of the device, including inexperienced and expert user populations
- An assessment of all components within the product that operate on the IoT system
- Unintended consequences of actuation of any type of energy release by users through remote control
- Unintended interactions of the subject device with other IoT devices
- Unintended consequences of various types of malfunctions, including failure to load a software updated, data or code corruptions, and unintended activation
- Unintentional defaulting to non-personalized settings
- Failure to operate one or more critical safety functions
- User error or misuse

Once a safety concern is raised through the risk assessment, the framework advises manufacturers to employ effective, feasible countermeasures, such as:

- Certification of critical components to the appropriate industry standard or rule
- Warnings and instructions to consumers
- User authentication and confirmation for activations
- Back-up systems for sensors or actuators that control safety devices
- Adequate information about device components so that product updates can be traced throughout the lifespan of the device

Recognizing that certain product types will necessitate added safety measures, the framework ends with providing an extensive list of special product types and their additional considerations. Some of the special product types and additional considerations included in the framework are:

- Wearable devices: information security and privacy breaches, potential for thermal burns, environmental isolation and potential distraction of users
- Home security and monitoring devices: information security and privacy breaches, reliability over the product lifespan, loss of connectivity
- Products connected to inherent hazards, such as stoves, fireplaces, and lawnmowers: accidental activation, intentional remote operation without presence of user, unintentional remote activation
- Products that respond to hazards, such as fire sprinklers and CO alarms: aging effects, false alarms, unintended activation leading to credibility questions
- Baby monitors and connected children's devices: information security and privacy breaches, thermal hazards, strangulation on cords

While this framework is detailed and should prove helpful to the consumer product safety community, Commissioner Kaye and Dr. Midgett emphasize in their framework that it is just the initiation of a necessary conversation about consumer product safety and IoT devices. The Mintz Consumer Product Safety team agrees, as there are other major IoT issues to be addressed by the safety community and the CPSC.

For example, not addressed in the framework is the implications of the separation of the consumer product manufacturer from the actual developer of the IoT technology. This may mean that the party who the CPSC considers as the product manufacturer of the IoT device may actually be a firm relying on a vendor, contractor, and/or subcontractor to develop IoT technology outside of the "manufacturers'" expertise. Because these new third parties will be developing the IoT technology, will they be relied upon for directly interfacing with the product and consumer? This structure will have important implications for how the CPSC monitors IoT devices and who it

communicates with when the agency addresses potential product hazards.

Then there are the myriad of CPSC practice and procedure issues. Should remedial software downloads be done unilaterally before receiving the CPSC's blessing on the remedy? Are public communications such as press releases necessary or even desirable if all customer problems can be repaired directly? How many years does a device's software have to be supported? If the software is no longer supported but results in a product safety issue, does the manufacturer have to take responsibility for the defect and report/recall in order to remedy the hazardous product?

These issues should be addressed in the near future before cases arise and policies are established by whatever companies are first in line. For now, we thank Commissioner Kaye and Dr. Midgett for taking the next step in the important conversation on IoT devices and consumer product safety.