Connected products can make the world a safer place: electronic sensors in the home can detect problems and send smartphone notifications to the homeowner; smart alert devices can notify family members or home help companies that an elderly person has fallen and needs assistance. But with over 64 billion connected products in the marketplace, there is a concern that connected devices could introduce hazards that might lead to a risk of injury due to problems with software updates or customization, faulty connections, and even consumer modifications.

As the body charged with overseeing consumer product safety in the U.S., over the last few years, the Consumer Product Safety Commission (CPSC) has shown an increasing interest in defining its role with regard to connected products. In May 2018, the CPSC held a public hearing on IoT, obtaining feedback from a range of stakeholders on potential risks of connected consumer products and the agency’s role. In late September, CPSC staff submitted to the Commission a status report outlining the CPSC’s work on consumer product IoT issues since the public hearing. The report also outlines how CPSC staff understands the agency’s role, which is safeguarding consumers from potential physical product risks, as well as how its work intersects with the jurisdiction of other agencies as they oversee connected products.
The report notes that this is an ongoing process, stating that CPSC staff is working on “how to define consumer product safety in terms of the IoT, the intersection of, and interdependencies among, consumer product safety, data security and privacy, and how our traditional risk management approaches apply to connected products.” The report acknowledges that privacy and data security are not within CPSC’s jurisdiction, but noted that at least one participant in CPSC’s 2018 hearing warned that “CPSC should pay attention to certain cybersecurity threats that create opportunities for physical harm, a risk not previously considered, and resist creating any prescriptive rules for IoT devices.”

To increase institutional knowledge of IoT benefits and challenges, CPSC has dedicated resources to develop its staff’s expertise. CPSC has also participated in developing voluntary standards, has taken a leadership role in establishing an interagency IoT working group, and has been developing its capability to simulate home networks at its laboratory.

The staff report outlines three ongoing internal projects relating to IoT. The first involves developing a methodology for assessing safety-related implications arising out of software and firmware updates to connected products. This project is at what CPSC views as the intersection of product safety and data security and potential “hazardization” of connected products as a result of data vulnerabilities. CPSC is also looking at connected heating appliances and the risks associated with their remote activation. Finally, CPSC is studying smart toys “in an effort to identify physical safety hazards.” It is surprising that CPSC staff would dedicate resources to toys as opposed to other products, like in-home safety devices, since the physical safety of toys is strictly regulated by the mandatory toy safety standard, ASTM F-963. The likelihood of physical hazardization of toys is far lower than, for example, connected home security devices and sensors. In those categories, connectivity, and thus security breaches that affect the operation of those devices, may be directly related to both safety risks and advantages. Indeed, home safety devices is a category where we have actually seen CPSC recall activity.

The report notes that CSPC is engaging in product safety assessments of connected& shared e-scooters. This is likely in response to reports of e-scooters that were vulnerable to hacking. The emerging hazards of micro-mobility devices such as shared e-scooters are also a focus of CPSC’s Operating Plan for Fiscal Year 2020 and represent another product category that appears to be more vulnerable to hazardization than connected toys.

CPSC staff intended to develop a best practices guide for industry and consumers on connected products, which was an enumerated project in the proposed Operating Plan for Fiscal Year 2020. However, an amendment introduced by Commissioner Feldman focuses CPSC’s resources on IoT intergovernmental work instead. Given the report’s acknowledgment that the agency is still working to develop staff expertise in IoT, attempting to create such a guide appears premature at this juncture.

The sharp increase in the number of connected devices in the market means it is necessary and appropriate for CPSC to continue to build expertise on IoT issues, even though very few examples of actual product safety hazards attributable to some type of connectivity failures exist. It would be useful for CPSC to focus its efforts and resources on product categories that pose a higher potential risk to the physical
safety of consumers through hazardization or failure as a result of connectivity, without overstating potential risks. It is encouraging that through the intergovernmental initiatives a variety of federal agencies are working collaboratively to better understand the various consumer protection issues potentially raised by connected products that fit within their respective jurisdictions.

© 2020 Keller and Heckman LLP