MAYER·BROWN

Legal Update
May 24, 2018

CPSC Considers Product Cybersecurity

Connected consumer devices—often referred to as the Internet of Things (IoT)—offer great economic opportunities for American businesses. This connectivity has enabled companies to offer exciting new products, enhance consumers' experience of existing products and monitor and improve device performance over time. Consumers are responding very positively, with rapid adoption of products from fitness trackers to connected fridges, streaming security cameras to smart speakers. Indeed, using connected consumer devices is quickly becoming the new normal at home and throughout consumers' daily lives.

These opportunities also come with new potential risks, including cyber threats to connected devices. IoT devices are exposed to potential data loss, ransomware and even the use of the devices to attack third-party systems. As a result, manufacturers, sellers and distributors of these devices face corresponding legal risks. For example, class action lawsuits have alleged that connected products were inadequately secured against cyber threats or violated user privacy. Likewise, US regulators including the Federal Trade Commission (FTC), National Highway Traffic Safety Administration (NHTSA) and Food and Drug Administration (FDA) have moved to regulate connected products within their jurisdiction.

Against this backdrop of increasing opportunity and legal risk in the IoT, the Consumer Product Safety Commission (CPSC or Commission) held a public hearing on May 16, 2018, to consider potential consumer product hazards posed by connected consumer devices. In this Legal Update, we first provide an overview of the CPSC's relevant authority, interest in the IoT and call for a hearing. Second, we discuss the following five key topics that were discussed at the hearing:

- Potential safety consequences of unique features of the IoT;
- Leveraging cyber risk management best practices from other contexts;
- The advantages of cyber risk management over prescriptive cyber regulation;
- Potential benefits of distinguishing between product categories; and
- The importance of regulatory coordination.

As discussed below, how the CPSC addresses these key issues over time is likely to be critical to how companies within the CPSC's authority should approach IoT cybersecurity and safety going forward. While we discuss these issues in the context of the CPSC, we note that in many respects the CPSC's areas of focus track those of other regulators (e.g. NHTSA, FDA). Businesses outside the CPSC's jurisdiction thus still may find that agency's approach to these issues instructive.

Background on the CPSC and Its Interest in the IoT

The CPSC: A Quick Primer: As its name indicates, the CPSC is focused on consumer product safety. Specifically, it has authority to

regulate the safety of "consumer products," a term that generally covers products sold or used by consumers, with certain exceptions for motor vehicles, food and other specified products.[1] Among other authorities, the CPSC may impose—and require manufacturers to certify to—performance requirements or disclosure requirements by rule when it is reasonably necessary to do so to prevent or reduce an unreasonable risk of injury associated with such product.[2] However, the CPSC is also expressly authorized by statute to rely upon voluntary standards when it is likely that there will be substantial compliance that will adequately reduce the risk of injury associated with a product.[3] The CPSC also has particular authorities that apply to children's products and toys,[4] may ban hazardous products that present risks that cannot be adequately addressed by any safety standard,[5] may bring a civil action for the condemnation and seizure of products that present an imminent and unreasonable risk of severe injury or death,[6] and may compel the recall of defective consumer products.[7] Violations of the prohibitions enforced by the CPSC can give rise to civil and criminal liability.[8]

The CPSC and the IoT: The CPSC has begun to prioritize emerging technologies, including the IoT, in recent years. Thus, the CPSC released a staff report in January 2017 that considered the impact of emerging technologies on consumer safety.[9] The report listed "[i]ncreased integration of smart technology and the Internet of Things" first on its summary list of factors "likely to influence the marketplace for consumer products." While the report acknowledged that data privacy is outside the jurisdiction of the CPSC, it focused on a wide range of connected consumer products. The report also suggested that the CPSC could itself leverage "Big Data," for example, to deliver safety messages to likely purchasers of certain products. It also recommended a series of possible policy steps for the CPSC to engage in going forward, including building internal "software engineering and evaluation skills" and partnering with other federal agencies when issues of "mutual concern" involve topics, such as data privacy, that are outside the CPSC's jurisdiction.

Hearing Notice: On March 27, 2018, the CPSC issued the notice for its recent hearing. It noted that "internet connectivity between products holds the promise of many benefits for consumers" but that it "is also capable of introducing a potential for harm (a hazard) where none existed before the connection was established."[10] The CPSC noted the range of consumer hazards that conceivably could be created based on the connected nature of IoT products, including because of potential remote operation, unexpected operating conditions, loss of a safety function and abuse of an intended product feature. The CPSC observed, however, that it does not "consider personal data security and privacy issues that may be related to IoT devices to be consumer product hazards that CPSC would address."

The CPSC thus framed a broad range of questions regarding IoT safety for consideration at the hearing, including ones relating to:

- The adequacy of voluntary standards to address safety hazards specific to IoT devices;
- Incidents involving IoT devices;
- Consumer education regarding proper use of IoT devices;
- Secure development practices for IoT devices; and
- Communication with consumers in recalls of IoT devices.

In the notice, the Commission also said it would accept written comments in connection with the hearing, with the comment period closing on June 15, 2018.

Key Topics Considered at the Hearing

The hearing consisted of three panels of witnesses representing a wide range of

stakeholders from industry, consumer groups and academia. With questions from Acting Chairman Ann Marie Buerkle and Commissioners Robert Adler, Elliot Kaye and Marietta Robinson, the hearing covered a broad range of topics relating to the potential consumer safety hazards posed by IoT devices. A handful of topics received particular consideration. These topics likely merit attention by businesses subject to the CPSC's authority—as well as by other businesses that are watching the CPSC to understand how its actions may inform actions taken by other regulators.

POTENTIAL SAFETY CONSEQUENCES OF UNIQUE FEATURES OF THE IOT

Product cybersecurity best practices draw in many respects upon those developed for managing cyber risks to *enterprise* systems. However, the hearing saw significant discussion of the unique features of the IoT that raise particular cyber risks. The discussion at the hearing made clear that companies subject to the CPSC's authority will be well-served to consider these unique challenges and risks as they work to secure IoT devices.

Most significantly, as the CPSC noted in its hearing notice and as was extensively discussed at the hearing, introducing connectivity into physical products creates potential risks of physical injury that do not need to be considered when securing a typical website or corporate database. A cyber attack that stops a smoke detector from functioning could lead to injuries in the event of a fire, just as could an attack that disables safety features built into a connected furnace. Likewise, cyber attacks on connected consumer devices could potentially lead to a risk of physical injuries, such as if an attack caused a connected toy or kitchen appliance to move in an unintended manner. Indeed, this link between IoT devices and potential physical harms was discussed throughout the hearing.

The hearing also considered a range of other distinctive features of the IoT such as:

- **The diverse products that comprise the IoT:** The hearing considered the broad range of consumer products that are being connected to the Internet. Hearing participants noted, for example, that some of these devices are being built with low-cost or low-power components that do not have strong built-in cybersecurity capabilities. Managing cybersecurity across this vast range of products, including their disparate supply chains and economic profiles, presents new challenges.
- **Challenges updating IoT devices:** Consumers have become accustomed to regular security updates to their computers and phones. In contrast, as discussed at the hearing, companies may have limited ability to push security updates to many IoT devices, at least in an economically feasible manner. Companies thus may face challenging questions about the extent to which they should provide security updates to products over time.
- **Challenges communicating with end users:** Consumers similarly have come to understand that computer or phone manufacturers will interact with them through the device about product-related issues. As highlighted at the hearing, however, many IoT devices lack an interface—making it important for companies to consider if and how they will provide any necessary communications to consumers.

LEVERAGING CYBER RISK MANAGEMENT BEST PRACTICES FROM OTHER CONTEXTS

The CPSC has a long history of addressing product defects and safety hazards with its own specific statutory authorities. Cyber risk management, which has its own distinct logic and vocabulary, has not traditionally been part of that work. Indeed, this was even literally true in the hearing notice: the word "cyber" does not appear in the Federal Register notice for the hearing. However, the hearing made clear that the Commission will be working to find

appropriate ways to integrate cybersecurity risk management principles into its approach to the safety of connected consumer products. For example, the hearing featured discussion on topics including:

- **Engaging with the cybersecurity community:** The hearing featured repeated calls for the CPSC to engage with the cybersecurity community. Witnesses urged the CPSC both to educate itself about cyber risk management for connected products and to give the cybersecurity community a better understanding of the CPSC's mission and priorities.
- **Leveraging existing cyber risk management frameworks:** The hearing saw discussion of the possibility of using existing cyber risk management frameworks—most notably, the NIST Framework—for managing risks to connected consumer products. The hearing did not answer what the precise content of such a framework should be. However, there were repeated calls for the development of comprehensive risk-based approaches to the security of connected consumer products. Likewise, the hearing covered familiar cyber risk management tools such as vulnerability assessments, penetration testing, security by design, coordinated vulnerability disclosure and risk assessment.

THE ADVANTAGES OF CYBER RISK MANAGEMENT OVER PRESCRIPTIVE CYBER REGULATION

The CPSC hearing featured extended discussion of a very familiar cybersecurity policy topic: the advantages of cyber risk management best practices over prescriptive regulations. The CPSC received testimony, for example, highlighting the significant challenges ahead of any attempt to create a cybersecurity performance standard to which manufacturers of connected devices would be required to certify. As discussed extensively at the hearing, such a performance standard would be at risk of creating prescriptive, static cybersecurity requirements that almost certainly could be bypassed by sophisticated hackers. Witnesses at the hearing instead argued that, consistent with cybersecurity best practices in other contexts, manufacturers should be free to identify the risks that actually face their products and develop risk-based measures to address those risks—without turning cybersecurity into a check-the-box exercise. Likewise, they argued that existing regulatory frameworks, such as rules governing toys, could not simply be expanded to cover new topics such as penetration testing for cyber vulnerabilities.

To be sure, this preference for a voluntary approach based on best practices was not unanimous. Some witnesses called for more extensive or prescriptive regulatory action, and there was some discussion of the creation of process-based standards or expectations for companies in this field. Moreover, the CPSC certainly could significantly shape how companies approach the cybersecurity of connected products even without establishing a performance standard. Nonetheless, the general tenor of the conversation indicated skepticism of using prescriptive rules to try to improve product cybersecurity. Whether the CPSC indeed is guided by such a skepticism of rule-based cybersecurity will be a critical issue for companies' approaches to compliance going forward.

POTENTIAL BENEFITS OF DISTINGUISHING BETWEEN PRODUCT CATEGORIES

As noted above, consumer IoT products fall into a wide range of product categories, from toys to home security systems to off-road vehicles. Discussion at the hearing reflected recognition that different types of products pose different types of risks and may be subject to different regulatory regimes. For example, multiple participants in the hearing generally characterized consumer IoT products as falling into three categories that could inform cyber risk management: (1) safety products (e.g., connected smoke detectors); (2) products that

could cause injury or death (e.g., connected furnaces); and (3) other products (e.g., connected toys). Likewise, participants observed that certain product categories are subject to distinct standards. For example, participants observed that connected toys are subject not only to the ASTM F963-17 standard, which the CPSC has incorporated, as modified, into governing regulations[11] but also to regulation by other agencies, such as by the FTC under the Children's Online Privacy Protection Act. Whether the CPSC decides to calibrate its regulatory approach based on these or other distinctions will likely be highly significant for businesses in this field going forward.

THE IMPORTANCE OF REGULATORY COORDINATION

As noted above, multiple regulatory agencies already have brought their unique perspectives and authorities to bear on the connected devices that comprise the IoT. The FTC has brought multiple enforcement actions targeting allegedly inadequate security or privacy practices in connected devices. The NHTSA has issued multiple pieces of cybersecurity guidance related to connected and autonomous vehicles. The FDA has issued pre-market and post-market guidance for the cybersecurity of medical devices. Moreover, the latter pair of regulators have both overseen recalls for connected products within their authority.

In light of this ongoing work by these and other agencies, the hearing featured repeated calls upon the CPSC to collaborate effectively with peer regulators in the United States and abroad to avoid inconsistent or duplicative approaches. While the details of such collaboration remain to be seen, the CPSC Commissioners appeared open to such collaboration and coordination.

Looking Ahead

The CPSC's hosting of a thorough and considered discussion of potential safety risks posed by connected products built effectively upon the Commission's 2017 staff report and suggests that the CPSC will take a thoughtful and serious approach to these important issues. Manufacturers of connected devices will benefit from following the CPSC's continuing work in this field as it adds to the ongoing regulatory scrutiny of the Internet of Things.

For more information section about the topics raised in this Legal Update, please contact any of the following lawyers.

Stephen Lilley
+1 202 263 3865
slilley@mayerbrown.com

Erika Jones
+1 202 263 3232
ejones@mayerbrown.com

Endnotes

[1] *See* 15 U.S.C. § 2052(a)(5).
[2] 15 U.S.C. § 2056(a) (rulemaking authority); 15 U.S.C. § 2063 (certification requirements).
[3] 15 U.S.C. § 2056(b).
[4] *See generally* 15 U.S.C. §§ 2056(a)-2056(b).
[5] 15 U.S.C. § 2057.
[6] 15 U.S.C. § 2061.
[7] 15 U.S.C. § 2064.
[8] 15 U.S.C. §§ 2069-2070.
[9] *See* CPSC, Staff Report, *Potential Hazards Associated with Emerging and Future Technologies* (Jan. 18, 2017).
[10] CPSC, The Internet of Things and Consumer Products Hazards, 83 Fed. Reg. 13,122 (Mar. 27, 2018).
[11] *See* 16 C.F.R. pt. 1250.

litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory and enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and private clients, trusts and estates.

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.