MERCATUS CENTER
George Mason University

Bridging the gap between academic ideas and real-world problems

PUBLIC INTEREST COMMENT

THE INTERNET OF THINGS AND CONSUMER PRODUCT HAZARDS

ADAM THIERER
Senior Research Fellow, Technology Policy Program, Mercatus Center at George Mason University

JENNIFER HUDDLESTON SKEES
Legal Research Associate, Technology Policy Program, Mercatus Center at George Mason University

ANNE HOBSON
Program Manager, Academic and Student Programs, Mercatus Center at George Mason University

Agency: US Consumer Product Safety Commission
Comment Period Opens: March 27, 2018
Comment Period Closes: June 15, 2018
Submitted: June 14, 2018
Docket No. CPSC-2018-0007

We appreciate the opportunity to respond to the request by the US Consumer Product Safety Commission (CPSC) for written comments on the potential safety issues and hazards associated with internet-connected consumer products. The internet of things (IoT) is a burgeoning ecosystem. Promoting resilience—that is, the capacity to withstand and learn from cyberattacks—in this ecosystem without hampering innovation is crucial for the ecosystem's full benefits to be realized.

IoT devices enhance productivity and convenience, helping to automate household chores from vacuuming to food preparation. The first recorded consumer IoT device was a Coca-Cola machine programmed in the 1980s by the Carnegie Mellon University Computer Science Department that used an internet connection to inform would-be drinkers about the status of its contents.[1] The added convenience ensured that students and professors didn't have to cross campus only to find an empty machine or a warm beverage. In the consumer market, the IoT gives users more instant control over devices such as TVs and thermostats. According to McKinsey Global Institute, the economic impact of household IoT applications will amount to $350 billion per year in 2025, cutting the time required for chores by 17 percent.[2] Additionally, the IoT industry will generate millions of job opportunities and trillions of dollars in both economic growth and cost savings.[3]

---

[1] Jordan Teicher, "The Little-Known Story of the First IoT Device," *IBM Industries Blog*, February 7, 2018, https://www.ibm.com/blogs/industries/little-known-story-first-iot-device/.
[2] James Manyika et al., *Unlocking the Potential of the Internet of Things* (New York: McKinsey Global Institute, June 2015).
[3] Adam Thierer and Andrea O'Sullivan, "Projecting the Growth and Economic Impact of the Internet of Things," Economic Perspectives, Mercatus Center at George Mason University, June 15, 2015.

For more information, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University
3434 Washington Blvd., 4th Floor, Arlington, VA 22201

Like many products, the IoT can be leveraged for beneficial or harmful ends. For example, botnets that harness the distributed computing power of connected devices may be used to disrupt major websites; yet the same technology may be used to raise money for charities or perform medical research.[4] Similarly, while software is key to the success of the digital economy, malware may damage computer systems. Thus, policymakers approaching the IoT must focus on preventing botnets and malware while avoiding efforts that make beneficial uses of software more difficult.

Our comments will emphasize developing a comprehensive, long-run approach to achieving a resilient IoT ecosystem. Resilience is the capacity to persist, adapt, learn, and recover from an adverse event. We argue below that a multistakeholder approach to the governance of the IoT is best suited to the dynamism and complexity of this ecosystem. By multistakeholder approach, we mean governance that involves government agencies as well as manufacturers, industry organizations, advocacy groups, researchers, and consumers in key decision-making. Focusing on resilience will minimize the safety risks associated with flaws or malfunctions in cyber-physical systems while promoting innovation in the consumer market.

THE LIMITATIONS OF RULEMAKING IN THE IOT ECOSYSTEM

The IoT is an array of connected, uniquely identified objects that are able to transfer data over a network.[5] These objects include emerging technologies such as smart speakers, autonomous vehicles, and drones, as well as more mature technologies such as smartphones and security cameras. There is a huge amount of variety in these devices. For example, not all IoT devices have sensors, but many do. Some devices are "always-on" (always connected to the internet), whereas some are intermittently connected. Some devices communicate only locally, whereas others have access to a larger network. Devices can be intended for consumer, industrial, or military use. Finally, devices can have intangible (digital) or tangible (physical) effects. Because of the variety in the IoT, a one-size-fits-all regulatory approach has a high potential for creating unintended consequences that hamper IoT development.

The breadth of the IoT ecosystem makes rulemaking and regulation regarding basic device design standards, certification programs, or required technical criteria particularly risky. It is important to understand the secondary effects of pursuing new requirements. Design standards can solidify inadequate or overly complex requirements and introduce costs that deter IoT innovation by redirecting labor and resources toward meeting regulatory compliance. In contrast, voluntary performance standards specify a desired outcome as opposed to dictating the way to achieve that outcome.[6] Performance standards more effectively align the incentives of companies and regulators because they reward activities directed at achieving security rather than specific compliance tasks that may or may not actually reach security goals.

---

[4] Charity Engine, "About Us," accessed June 1, 2018, http://www.charityengine.com/about; Folding@Home, home page, accessed June 1, 2018, http://folding.stanford.edu/.
[5] Anne Hobson, "Aligning Cybersecurity Incentives in an Interconnected World" (R Street Institute Policy Study No. 86, R Street Institute, Washington, DC, February 2017).
[6] David Hemenway, *Performance vs. Design Standards* (Washington, DC: US Department of Commerce, National Bureau of Standards, October 1980), 1–35.

It is important to be specific about the devices to which safety standards apply. For example, the state legislature of California proposed an early draft of a bill targeting all IoT devices that required manufacturers to "design the device to indicate when it is collecting information."[7] However, for always-on devices such as autonomous vehicles, smartphones, or digital assistants, this indicator loses its meaning. IoT devices fall into dozens of overlapping categories depending on the prevalence of certain features and differences in use cases. Furthermore, use cases may change over time. For example, smartphones are cameras and recording devices, and are even becoming personal assistants. Home assistants may now serve predominantly as timers, music players, and online shoppers, but will soon commonly be connected with HVAC systems, doorbells, and laundry machines. The changing landscape of use cases and potential threat vectors can cause standards to be easily outdated.

A truly resilient IoT ecosystem requires that stakeholders have the ability to adapt and learn from failures and mistakes. Compliance tasks resulting from poorly implemented standards or certifications can introduce complacency, foster a false sense of security in the face of evolving threats, and compromise an organization's or individual's ability to learn how to recover from and respond to threats.

In order to meet the challenge of large-scale cyber insecurity, federal agencies should empower stakeholders at multiple levels to persist in their efforts to develop and adopt new technologies, and these agencies should not be deterred by cybersecurity threats and attacks. Industry groups and agencies should constantly update guidelines to adapt to emerging threats. Small and large manufacturers should invest in cyber insurance and adhere to the National Institute of Standards and Technology (NIST) guidelines to manage risk. Consumers groups can develop certification programs and can complement agencies in educating consumers about cyber threats. In general, federal agencies should empower stakeholders by giving them the space to develop solutions.

For systems to endure and function under and after cyberattacks, stakeholders must be able to have at their disposal multiple pathways of response so that no single vulnerability disrupts the operation of the entire system. In order to allow for those multiple pathways of response to be available, a multifaceted approach to governance should include industry-led standards, voluntary certification programs, cyber-insurance adoption, increased use of guarantees and warranties, and education of consumers.

Some cybersecurity solutions in the IoT already exist and are pursued by federal agencies, international bodies, industry groups, and third parties. In 2016, Underwriters Laboratories launched a Cybersecurity Assurance Program,[8] providing certifications to products that meet testable criteria. Voluntary premarket or postmarket certifications can also provide consumers with the necessary certainties to make informed choices about what devices they purchase and promote best practices within the industry. This has been seen in other industries, such as with the Green Building Initiative.[9]

---

[7] S.B. 327, 2018 Leg., 2017–18 Sess. (Cal. 2018).
[8] UL, "UL Launches Cybersecurity Assurance Program," news release, April 5, 2016, https://www.ul.com/newsroom/pressreleases/ul-launches-cybersecurity-assurance-program/.
[9] John J. Kirton and Michael J. Trebilcock, eds., *Hard Choices, Soft Law: Voluntary Standards in Global Trade, Environment, and Social Governance* (London: Routledge, 2004); US Green Building Council, "About USGBC," accessed June 1, 2018,

Efforts also include the development of flexible guidelines such as the NIST Cybersecurity Framework,[10] the Online Trust Alliance's Trust Framework,[11] and 30 other standards of varying technical specificity and focus from groups such as the International Organization for Standardization, Institute of Electrical and Electronics Engineers, and the Internet Engineering Task Force.[12] The NIST framework provides a common language for cybersecurity risk management. It characterizes the various levels of investment in cybersecurity that organizations currently adopt to manage threats—ranging from simple awareness to having adaptive systems. The framework also groups specific implementation measures across five large risk-management functions: identifying threats, protecting systems, detecting threats, responding to threats, and recovering from attacks. The CPSC should be involved with efforts to update and expand the NIST framework and encourage its adoption among manufacturers of consumer products. Furthermore, rather than starting its own certification program or standards efforts, the CSPC should collaborate with entities already pursuing solutions to cyber insecurity. For example, the Consumer Technology Association (CTA) created a security checklist for sellers and manufacturers of household connected devices.[13] These groups have already developed industry practices and norms that should be considered in any potential regulatory or guidance-related measures. The CPSC can work with industry groups to create voluntary guidelines or checklists for vendors that focus specifically on implications for physical safety in the IoT ecosystem. Working with such groups would produce positive collaborative consensus for consumer safety.

The CPSC should also encourage industry adoption of a growing range of cyber insurance offerings. The process of acquiring cyber insurance involves cyber risk assessments. The insured parties are incentivized to become aware of vulnerabilities and put basic cyber practices in place to receive lower premiums.[14] Basic cyber practices can include shipping devices with up-to-date software, allowing users to change device passwords, employing strong authentication and cryptography best practices, and testing device configurations.[15] Currently, the manufacturing sector lags the healthcare and financial services sectors in insurance uptake.[16]

The IoT is a complex and ever-changing global ecosystem. The role of the CPSC and other agencies in addressing cyber insecurity is to foster the ecosystem's ability to adapt and learn. This requires an approach that emphasizes resilience as the end goal.

---

https://new.usgbc.org/about; Marine Stewardship Council, "Sustainable Seafood: The First 20 Years: A History of the Marine Stewardship Council," accessed June 1, 2018, http://20-years.msc.org/.

[10] National Institute of Standards and Technology, "Cybersecurity Framework," accessed June 1, 2018, https://www.nist.gov/cyberframework.

[11] Online Trust Alliance, "OTA Releases IoT Trust Framework," press release, March 2, 2016, https://otalliance.org/news-events/press-releases/ota-releases-iot-trust-framework.

[12] National Telecommunications and Information Administration, Existing Standards, Tools and Initiatives Working Group, *Catalogue of Existing IoT Security Standards*, n.d.

[13] Consumer Technology Association, "Device Security Checklist," accessed June 1, 2018, https://www.cta.tech/Membership/Member-Groups/TechHome-Division/Device-Security-Checklist.aspx.

[14] Hobson, *Aligning Cybersecurity Incentives*.

[15] Broadband Internet Technical Advisory Group, *Internet of Things (IoT) Security and Privacy Recommendations: A Broadband Internet Technical Advisory Group Technical Working Group Report*, November 2016.

[16] Council of Insurance Agents and Brokers, *Cyber Insurance Market Watch Survey: Executive Summary*, 2017.

FAVORING A RESILIENCE APPROACH RATHER THAN A PRECAUTIONARY APPROACH

The CPSC should take an approach that encourages and collaborates with existing efforts to make the IoT ecosystem more secure. The resilience approach to the IoT requires bottom-up, distributed efforts from all stakeholders. It recognizes that IoT technology improves existing consumer products but also improves safety overall.[17] These devices will promote an overall improvement in the safety and standard of living for many and will be able to develop more quickly in the absence of unnecessary regulatory barriers.[18] In general, the common law and consumers should be left to determine the appropriate level of safety in products on the market. Regulatory intervention should be reserved for those cases where the harm is highly probable, tangible, immediate, irreversible, and catastrophic.[19] It is highly unlikely that consumer IoT devices would result in this type of harm.

To date, we could not find recorded incidents of the use of household consumer products resulting in physical harm to consumers or their property as a result of their internet-connected nature. While the potential for consumer products causing physical harm to consumers or their property has been demonstrated in closed settings,[20] a precautionary approach involving new security baselines or certification program is not necessary at this point, and it could in fact prove harmful. This is especially true for IoT products where an overabundance of caution may result in establishing a duty that would not have otherwise existed.

Furthermore, current CPSC standards, including ASTM F963, and existing regulations, such as the Children's Online Privacy Protection Act, already prevent against hazards resulting from inadequate safety and data security protections for connected toys and devices marketed to children.[21] The CPSC must resist the urge to develop a "theory of everything" that would trade innovation for a false sense of having avoided risk. Instead, it should embrace a ground-up development of best practices and pursue additional actions only on a case-by-case basis and limited to the narrow applications necessary.

The CPSC should embrace an approach that emphasizes innovation and encourages self-governance. In a policy environment that promotes resilience as an end goal, creators are likely to develop safety processes and measures that appeal to consumers' actual preferences and not merely their expressed ones. For example, many consumers say they value their privacy, but few choose to change their behavior or take additional steps to protect information they reveal online.[22] Consumers select different blocking and screening technologies for websites, and similar features are developing in the IoT market. Consumers exhibit many different safety and security preferences. The CPSC should consider that despite consumers expressing a desire for increased

---

[17] Geoff Wheelwright, "IoT-Linked Wearables Will Help Keep Workers Safe," *Financial Times*, October 17, 2017.
[18] Cliff Saran, "Realising the Benefits of a Totally Connected World," *Computer Weekly*, December 2013.
[19] Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington, VA: Mercatus Center at George Mason University, 2014), 4.
[20] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—with Me in It," *Wired*, July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
[21] ASTM International, "ASTM F963 - 17: Standard Consumer Safety Specification for Toy Safety," accessed June 1, 2018, https://www.astm.org/Standards/F963.htm; Federal Trade Commission, "Children's Online Privacy Protection Rule ("COPPA")," accessed June 1, 2018, https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.
[22] Tom Hall and Kathleen Cahill, "The Privacy Paradox: We Say We Value It. What We Do Online Suggests Otherwise," *WYPR*, May 9, 2017.

privacy, they are often unwilling to deal with the accompanying inconveniences.[23] As a result, it is important to consider limiting the number of default requirements to truly catastrophic cases, and instead encouraging the development of optional privacy and security settings that consumers may opt into or out of as fits their needs.[24]

The CPSC should participate in existing multistakeholder processes for developing standards and certifications. Initiatives that include industry representatives, regulators, and consumer groups will ensure that the technology is developed in a way that preserves the desired consumer experience. In general, a soft-law, multistakeholder approach is more likely to result in the desired results without sacrificing the potential development of better, safer products for consumers.[25] Soft law refers to informal and flexible rulemaking, as opposed to the strict, formal rules of statutes and administrative regulations. Because of the tentative and provisional nature of soft law, regimes governed by soft law allow a wider variety of methods to be proposed and tested, resulting in systems that are less uniform, more decentralized, and less vulnerable to systemic threats.[26]

CPSC'S ROLE AS A CONSUMER EDUCATOR

We believe there is a role for the CPSC in educating and empowering consumers. When physical harm does occur, the CPSC can draw attention to recalls. The CPSC can also work with the affected company to leverage the IoT to notify consumers of the nature of the harm through push notifications or other forms of notice. It is important to focus on identifiable IoT-related harms rather than potential or hypothetical harms to avoid warning fatigue or unnecessary precaution. In this way, the IoT can be a boon for getting critical information to consumers.

There is also a growing set of IoT devices and services intended to mitigate some of the common problems with other consumer IoT devices. For example, smart firewalls and routers can track network traffic within a home, identifying malware or flagging patterns in traffic that reflect malicious botnet activity.[27] Larger consumer awareness of these products could improve baseline cybersecurity and hold manufacturers responsible. Online feedback mechanisms such as product reviews and ratings are already effective ways consumers and consumer groups can warn others about flawed products. Similarly, brands and reputations will develop over time. Increased use of warranties and guarantees related to cybersecurity can help boost consumer trust and provide a mechanism to hold manufacturers accountable.[28]

Consumers, when they know about poor data security practices, can be effective advocates for change. For example, after a DDoS attack in November 2016 in which the Mirai malware infected hundreds of thousands of IoT devices, the Chinese company responsible for manufacturing the webcams implicated in the attack voluntarily recalled millions of insecure devices to avoid the

---

[23] Alan McQuinn, "The Economics of 'Opt-Out' versus 'Opt-In,'" *Innovation Files*, October 6, 2017.
[24] McQuinn, "The Economics of 'Opt-Out' versus 'Opt-In.'"
[25] Ryan Hagemann, Jennifer Skees, and Adam Thierer, "Soft Law for Hard Problems: The Governance of Emerging Technology in an Uncertain Future," *Colorado Technology Law Journal* (forthcoming).
[26] Hagemann, Skees, and Thierer, "Soft Law for Hard Problems."
[27] Anne Hobson, "Cybersecurity in the Internet of Things Is a Game of Incentives," *The Hill*, Jan 19, 2017.
[28] Anne Hobson and James Czerniawski, "What the Internet of Things Can Learn from Used Cars," *Real Clear Future*, July 17, 2017.

scorn of the public and other entities.[29] We believe that the CPSC can play a complementary role in helping to inform consumers of incidents and recalls when necessary.

UTILIZING MULTISTAKEHOLDER PROCESSES AND OTHER COLLABORATIVE GOVERNANCE AS AN ALTERNATIVE TO TRADITIONAL REGULATION

As part of an overall approach to fostering resilience against cyber threats in IoT technologies, the CPSC should consider continuing the collaborative governance, or soft law mechanisms, rather than a more formal hard law approach of mandatory rules and restrictions. The CPSC can follow the example and collaborate with agencies like the Federal Trade Commission (FTC), the Food and Drug Administration (FDA), NIST, and National Telecommunications and Information Administration (NTIA), which have already worked with industry innovators and civil society leaders to develop informal standards and norms on topics like privacy and security. On the potential for malfunction related to IoT devices that include radios, the CSPC should communicate with the Federal Communications Commission (FCC). The Department of Homeland Security (DHS) plays a critical role in coordinating cybersecurity efforts across the federal government with a focus on risk management and resilience.[30] By focusing on collaborative, informal processes that are adaptive to new innovations in this space, the CPSC will be more likely to create an environment that allows consumers access to safe products without sacrificing innovation.

The FTC and NTIA have already conducted multistakeholder processes related to IoT devices and have generated best practices and norms through which the private sector has been able to engage in self-regulation to a large degree, with the government minimally formalizing the norms that emerge from such discussions.[31] NTIA's green paper on IoT development defines an appropriate role for government as supporting emerging technologies.[32] As the Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team pointed out in a 2017 green paper, the framework of allowing the private sector to lead in technology advancement and engage in collaborative processes when needed should work well for the IoT, as it did for the development of the original internet.[33] The CPSC should work collaboratively with these departments that have already engaged in collaborative discussions on these issues, rather than issue additional requirements that may result in fewer of the products or innovations that might actually make the technology safer for consumers.

Existing working groups at the NTIA have already established best practices for a wide variety of issues such as security upgradability and patching of devices.[34] The CPSC should draw on these

---

[29] Michael Mimoso, "Chinese Manufacturer Recalls IoT Gear Following Dyn DDoS," *Threat Post*, October 24, 2016.
[30] US Department of Homeland Security, *Cybersecurity Strategy*, May 15, 2018.
[31] Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World*, January 2015; National Telecommunications and Information Administration, "Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching," November 7, 2017, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security; Hagemann, Skees, and Thierer, "Soft Law for Hard Problems."
[32] US Department of Commerce, Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things*, January 2017.
[33] Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things*, 11; Ryan Hagemann, "Green Paper: Fostering the Advancement of the Internet of Things" (Public Interest Comment, Niskanen Center, Washington, DC, February 8, 2017).
[34] 81 Fed. Reg. 64139 (September 19, 2016).

groups' recommendations in determining if any further safety or security is necessary. These working groups have shown an ability to focus on both industry and consumer needs in a way that is able to dive deeper and result in more practical consensus than a top-down regulatory approach would. Additionally, the reliance on working group recommendations as opposed to harsher, more formalized rulemaking allows for such recommendations to more easily account for new concerns or adapt to changes in other regulatory schemes or issues.

Generally these groups are able to engage in a more democratic process that results in a voluntary, self-regulatory format that balances private industry interests with the government's desire to protect the public interest.[35] These processes also insure that regulatory bodies are able to learn from expertise in the industry rather than relying on their own internal and often outdated knowledge of the industry.

Approaching these problems through a soft law, collaborative governance framework does not mean that other policy mechanisms shouldn't exist. Consumer smart products are subject to the same safety standards as their nonsmart counterparts; likewise, they are subject to the FTC Section 5 unfair and deceptive trade practice standards for their claims. The FTC took D-Link to court for shipping routers and internet cameras with default passwords despite their claims of advanced network security.[36] With these existing standards in mind, the CPSC should consider the potential for conflicting regulation to give rise to uncertainty and result in less innovation and lower-quality products.[37]

LIABILITY QUESTIONS IN CONSUMER SAFETY AND THE IOT

Not only are consumer products already subject to safety regulations and requirements through other agencies, there are already safety standards for most traditional products now connected via the IoT. Additionally, the common law surrounding product liability provides certain de facto regulations, owing to the threat of liability should a problem arise.[38] Unless the introduction of an IoT element fundamentally changes a product by increasing or decreasing the safety, then it is unlikely additional safety standards need generally be established. The CPSC should avoid establishing broad regulations that do not account for the diversity of technologies captured by the term "internet of things." At the same time, the CPSC must also be careful not to regulate too narrowly and target a useful technology before its potential advantages are known.

In most cases, the CPSC should allow common-law products liability to apportion fault. If the CPSC or other regulators step in, it should be to limit the liability of internet-enabled devices for injuries that are not caused by the innovation but by a more traditional product. In determining whether the internet-connected element is associated with the injury, the CPSC should look at whether the injury would have occurred without the connected element. In such situations, the responsibility and liability should rest only on the traditional product. The CPSC has experience

[35] Hagemann, Skees, and Thierer, "Soft Law for Hard Problems."
[36] Federal Trade Commission, "FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras," press release, January 5, 2017, https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.
[37] Philip K. Howard, "Radically Simplify Law," *CATO Online Forum*, November 12, 2014.
[38] Alexandra B. Klass, "Tort Experiments in the Laboratories of Democracy," *William and Mary Law Review* 50 (2009): 1508–9.

making such distinctions between component parts and the finished product for other consumer products that use new technologies.[39]

When adding a third-party internet-enabled element to an existing product, the original product manufacturer should simultaneously be relieved from liability for any harm caused by the device and should not be held responsible for violations of existing standards that were caused by the technology and not the original product. Many states have adopted substantial modification as a defense to products liability claims, and the CPSC's regulations should follow suit.[40]

To effectively protect consumer safety, the CPSC must be careful that any safety regulations regarding IoT devices address only the part actually at risk of causing harm. Rather than raising the regulatory burden on both standard and IoT devices, the CPSC should consider lowering burdens on all devices as technological advances make them safer.[41]

CONCLUSION

We applaud the CPSC's efforts to examine questions about the safety of connected devices as this technology rapidly evolves, and to consider the framework that will encourage consumer trust in these new products' safety while still encouraging innovation in this area. We encourage the CPSC to take a flexible approach that fosters resilience, respects the complexity and dynamism of the IoT, and embraces a multistakeholder process. The CPSC should draw on the recent experiences of other bodies interacting with IoT technology and carefully consider if any additional regulations would improve consumer safety.

The CPSC is unique in its focus of communicating with consumers about harms associated with consumer devices. Accordingly, the CSPC should leverage IoT technology to educate and empower consumers about incidents of physical harm or product recalls. In this rapidly changing field, a flexible approach that minimizes bureaucratic requirements is likely to achieve results that protect both consumers and innovation. The right policy environment will allow a wide set of solutions to evolve, improving cybersecurity and safety outcomes for consumers of internet-connected products.

[39] Conditions and Requirements for Relying on Component Part Testing or Certification, or Another Party's Finished Product Testing or Certification, to Meet Testing and Certification Requirements, 16 C.F.R. 1109 (2012).
[40] Jones v. Hittle Services, 549 P.2d 1383 (1976).
[41] Adam Thierer, "Converting Permissionless Innovation into Public Policy: 3 Reforms," *Plain Text*, November 29, 2017.