Testimony of Katie McInnis for the Maryland Senate Hearing on the Security Features for Connected Devices

Before the Senate Finance Committee

February 19, 2020

SB 0443 and HB 888—SUPPORT WITH AMENDMENTS
Katie McInnis, Policy Counsel, Consumer Reports, Inc.

Thank you Chair Senator Delores G. Kelley and Vice Chair Senator Brian J. Feldman for this opportunity to speak with you today about the SB 443—Security Features for Connected Devices. My name is Katie McInnis and I serve as a policy counsel for the advocacy division of Consumer Reports.

Consumer Reports is an independent, nonprofit member organization. We use our rigorous research, consumer insights, journalism, and policy expertise to inform purchase decisions, improve the products and services that businesses deliver, and drive regulatory and fair competitive practices. Americans have a fundamental right to privacy and this bill takes important steps to protect this critical liberty.

We are glad to see the Maryland Legislature engaged on the issue of insecure connected devices. Connected devices are increasingly used in the home and collect highly sensitive information such as audio and video recordings. Many of these devices are built without adequate security, allowing, for instance, open viewing of home security systems and baby monitor feeds. In order for consumers to use these products with confidence, manufacturers must take reasonable measures to ensure that the data the device collects is secure. However, as written, the bill would not fully guarantee those protections.

We appreciate that Maryland Senators and Delegates are interested in better protecting the security of consumers' devices. But the bill should be improved so that it ensures an adequate standard of security for consumers. This is particularly important because these devices are growing in popularity, leaving more and more consumers vulnerable to security breaches. Consumer Reports recommends several changes:

- Remove the language that could give the impression that unique passwords constitute reasonable security;
- Expand the definition of connected devices to cover all of the protocols currently in use; and

- Augment the reasonable security requirement so that manufacturers are required to keep security features up-to-date for the reasonable lifetime of the device.

First, the bill suggests that passwords constitute reasonable security; this language should be removed. Passwords are easily foiled and should not be considered reasonable security. As told to Gizmodo by security expert Bruce Marshall: "There are a ton of ways your password can be exposed. . . They include someone simply guessing it, using a phishing attack to make you enter it into a compromised site, or using a brute-force attack to try a huge number of combinations in rapid succession (which many apps and sites will now stop from happening)."[1] And according to CSO, it's time for companies to move beyond passwords. "Password-only protection is permanently broken, and any organization relying on it is placing its business and reputation at risk."[2]

It's important that the reasonable security language be less prescriptive so that businesses can adapt their security techniques to respond to new threats. Maryland's existing data security requirement, which requires reasonable security,[3] reflects this, as do data security statutes around the country.[4] As noted above, it's likely that manufacturers will move away from password protection as they find more reliable means of authentication, leaving the current SB 443/HB 888 language outdated. For companies seeking more guidance, there are a number of security standards available; Consumer Reports has helped develop the Digital Standard for this purpose.[5] Any company that could show that it adhered to one of these standards could have a reasonable defense against claims of wrongdoing.

Second, all connected devices should be covered by this legislation. While the existing bill is currently limited to devices with IP addresses and Bluetooth, there are a wide variety of protocols that should be covered. For example, researchers were able to hack into devices running on ZigBee protocol;[6] and white-hat hackers were able to break into Z-Wave devices.[7] Moreover, carving out these various protocols will incentivize manufacturers to use these unregulated protocols, making devices even less secure. All connected devices should be required to be secure.

---

[1] David Nield, *Why Your Passwords Aren't Strong Enough—And What To Do About It*, GIZMODO (Mar. 29, 2018), https://gizmodo.com/why-your-passwords-arent-strong-enough-and-what-to-do-a-1823684095.

[2] Michael Nadeau, *Ready for More Secure Authentication? Try These Password Alternatives and Enhancements*, CSO (June 8, 2018), https://www.csoonline.com/article/3237827/ready-for-more-secure-authentication-try-these-password-alternatives-and-enhancements.html.

[3] MD. CODE COM. LAW §14-3503(a).

[4] *Data Security Laws, Private Sector*, NAT'L CONF. OF STATE LEGISLATURES (May 29, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[5] Digital Standard, https://www.thedigitalstandard.org/ (last visitedFeb. 18. 2020).

[6] Thomas Ricker, *Watch a Drone Hack a Room Full of Smart Lightbulbs from Outside the Window*, THE VERGE (Nov. 3, 2016), https://www.theverge.com/2016/11/3/13507126/iot-drone-hack.

[7] Thomas Brewster, *A Basic Z-Wave Hack Exposes Up To 100 Million Smart Home Devices*, FORBES (May 24, 2018), https://www.forbes.com/sites/thomasbrewster/2018/05/24/z-wave-hack-threatens-to-expose-100-million-smart-homes/.

Finally, it's important to require manufacturers to keep security features up-to-date throughout the reasonable lifetime of the device, because outdated and unpatched software is one of the most common causes of security breaches. According to security expert Bruce Schneier, writing in Wired, there are "[h]undreds of millions of devices that have been sitting on the Internet, unpatched and insecure, for the last five to ten years."[8] He cites this as one of the causes of the "crisis" of IoT insecurity. Not only would this requirement improve security, it would also help avoid planned obsolescence—so that consumers aren't forced to buy a new device once a company decides to stop updating the software.

Adequate security standards are particularly important because so many of these products are targeted to children. Indeed, research on connected toys and smartwatches designed for children has exposed serious data security vulnerabilities, allowing nefarious actors to spy on children or access their geolocation. For instance, with the My Friend Cayla doll, an individual could use the unsecured device to listen to the child playing with the doll.[9] In an even more concerning case, research found that children's smartwatches were built without sufficient security measures, allowing a stranger to track and communicate with the child wearing the watch.

Maryland residents need strong data security for their connected devices. We urge you to support amendments that improve this bill so that it appropriately protects consumers' connected products. Finally, we would like to thank the Committee for considering a bill to help the security of Marylanders' connected products.

[8] Bruce Schneier, *The Internet of Things is Wildly Insecure—And Often Unpatchable*, WIRED (Jan. 6, 2014), https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

[9] *See Internet-Connected Toys Are Spying on Kinds, Threatening Their Privacy and Security*, CONSUMER REPORTS (Dec. 6, 2016), https://advocacy.consumerreports.org/press_release/internet-connected-toys-are-spying-on-kids-threatening-their-privacy-and-security/.