April 13, 2022

The Honorable Jesse Gabriel, Chair
Privacy and Consumer Protection Committee
Room 162, Legislative Office Building
1020 N. Street
Sacramento, CA 95814

Re: AB 2392 Information privacy, connected devices (Irwin) — Oppose unless amended

Dear Chair Gabriel,

Consumer Reports[1] writes to share concerns about AB 2392, which would add a new safe harbor to the state's requirement to keep the data of internet-connected, or "Internet of Things" (IoT) devices secure. Internet-connected devices like smart speakers and cameras are growing in popularity, leaving more and more consumers vulnerable to security breaches. In 2018, California adopted a first-of-its-kind law requiring manufacturers to adopt reasonable security procedures to keep IoT devices protected from hackers.[2] Unfortunately, because the 2018 measure already included a safe harbor for enabling a device with a password — even though passwords are just one element of reasonable security — existing law does not adequately protect the security of these devices.

This bill, AB 2392, proposes to add a new safe harbor to the IoT security requirement — for compliance with the recent National Institute of Standards and Technology (NIST) labeling framework — compounding the problems with the existing law. Neither safe harbor is suited to constitute reasonable security. At the very least, we recommend replacing the existing safe

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

[2] SB 327/AB 1906 (2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327. Oregon passed a similar law the following year; only these two states currently have a data security requirement for internet-connected devices. *See*, David Stauss et al., *Two New State IoT Laws Go into Effect on January 1,* Byte Back (Oct. 27, 2019), https://www.bytebacklaw.com/2019/10/two-new-state-iot-laws-go-into-effect-on-january-1/.

harbor for unique passwords in Cal. Civ. Code § 1798.91.04(b) with a stronger safe harbor, similar to the one proposed in this bill, but adjusted to account for updates to the NIST document.

First, lawmakers must remove the safe harbor in Cal. Civ. Code § 1798.91.04(b) for new or unique passwords. Passwords can be accessed or circumvented, and they should not by themselves be considered reasonable security. It is easy to set up a unique-password remote connection while leaving devices unsecured. Gizmodo points out how easy it is for attackers to obtain your password, including by "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)."[3] And according to CSO, "Password-only protection is permanently broken, and any organization relying on it is placing its business and reputation at risk."[4]

This bill proposes to add a new safe harbor, but this fails to address the underlying problems with the law. And because the proposed safe harbor is so specific, it is likely to be outdated fairly quickly. Under the bill, the security requirement is satisfied if a third party assesses that the manufacturer of a connected device meets the baseline criteria of NIST's Feb. 4, 2022 Cybersecurity White Paper, "Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products," and the product is labeled as such.[5] This is stronger than the existing safe harbor, including because it requires obtaining a third-party assessment for adherence to the security criteria, as well as a labeling requirement to help guide consumers. But the existing safe harbor still remains, and further, using a specific, dated paper as a safe harbor for compliance means that it could become outdated as technology changes. Data security language should be flexible so that businesses can adapt their security techniques to respond to new threats. Data security statutes around the country, including California's security requirement for data owned, licensed, or maintained by a business, reflect this.[6]

Of course, a safe harbor isn't necessary at all: for companies seeking more guidance, there are a number of security standards available; Consumer Reports has helped develop the Digital Standard for this purpose.[7] Any company that could show that it adhered to one of these standards could have a reasonable defense against claims of wrongdoing.

---

[3] 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.
[4] *Michael Nadeau, 6 password alternatives and enhancements*, CSO (Jun 8, 2018), https://www.csoonline.com/article/3237827/ready-for-more-secure-authentication-try-these-password-alternatives-and-enhancements.html.
[5] *Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products*, National Institute of Standards and Technology (Feb. 4, 2022), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf.
[6] Cal Civ. Code § 1798.81.5; *Data Security Laws | Private Sector,* National Conference of State Legislatures (May 29, 2019), https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.
[7] The Digital Standard, https://thedigitalstandard.org/.

It's important to get this right, because there's a lot at stake. Without meaningful security requirements, IoT devices are very vulnerable to data breaches. 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.[8] 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.

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.[9] For instance, with the My Friend Cayla doll, an individual could use the unsecured device to listen to the child playing with the doll. 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.

Therefore, we recommend several additional steps to build on existing law:

- Expand the definition of connected devices to cover all of the protocols currently in use;
- Augment the reasonable security requirement so that manufacturers are required to keep security features up-to-date for the reasonable lifetime of the device; and
- Clarify that, where possible, "smart" or connected devices should still work if they stop getting security updates, and as a result, lose internet connectivity.

We discuss these recommendations in more detail below.

Expand devices covered by the law. All connected devices should be covered by a data security requirement. Existing law is currently limited to devices with IP addresses and Bluetooth, but there are a wide variety of protocols that should be covered, especially as smart home devices often run on these other protocols. IoT Times lists several, including ZigBee;[10] other lists are

[8] *FTC Approves Final Order Settling Charges Against TRENDnet, Inc*., Fed. Trade Comm'n (Feb. 7, 2014), https://www.ftc.gov/news-events/press-releases/2014/02/ftc-approves-final-order-settling-charges-against-trendnet-inc, and see *ASUS Settles FTC Charges that Insecure Home Routers and "Cloud" Services Put Consumers' Privacy at Ris*k, Fed. Trade Comm'n (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put.

[9] *Internet-Connected Toys are Spying on Kids, Threatening their Privacy and Security*, Consumers Union (Dec. 6, 2016), https://consumersunion.org/news/internet-connected-toys-are-spying-on-kids-threatening-their-privacy-and-security/; *Consumers Union Renews Call for FTC to Investigate Reports of Security, Privacy Concerns with Smartwatches for Kid*s, Consumers Union (Dec. 7, 2017), http://consumersunion.org/news/consumers-union-renews-call-for-ftc-to-investigate-reports-of-security-privacy-concerns-with-smartwatches-for-kids/.

[10] Pablo Valerio, *Top wireless standards for IoT devices*, IoT Times (Apr. 11, 2018), https://iot.eetimes.com/top-wireless-standards-for-iot-devices/.

even more extensive.[11] Researchers were able to hack into devices running on ZigBee protocol;[12] white-hat hackers were able to break into Z-Wave devices.[13] Moreover, carving out these various protocols will incentivize manufacturers to use these unregulated protocols, making devices even less secure.

Require security updates. Next, it's important to require manufacturers to keep security features up-to-date for the reasonable lifetime of the device. Otherwise, businesses have too much leeway to stop supporting these devices, inappropriately shortening the lifetime of the device — forcing consumers to throw it away and buy a new one, which can be costly and wasteful.[14] In addition, devices with outdated and unpatched software are commonly subject to security breaches. According to Bruce Schneier, there is a "crisis" of IoT insecurity, in part because of the "[h]undreds of millions of devices that have been sitting on the Internet, unpatched and insecure, for the last five to ten years."[15]

Smart devices should work without connectivity. Finally, as pointed out by the Federal Trade Commission, consumers expect that "smart" devices that no longer receive support, such as security updates, would have a longer lifetime as conventional devices and continue to work without connectivity.[16] For example, if possible, a connected toaster should still work as a toaster even after its connectivity is disconnected.

We would be happy to provide language suggestions. Thank you for your consideration. We look forward to working with you to ensure the strongest possible protections for consumer data.

Sincerely,

Justin Brookman
Director, Technology Policy

---

[11] *The Complete List of Wireless IoT Network Protocols*, LinkLabs (Feb. 8, 2016), https://www.link-labs.com/blog/complete-list-iot-network-protocols.
[12] 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.
[13] 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/.
[14] Romain Dillet, *Sonos clarifies how unsupported devices will be treated*, TechCrunch (Jan. 24, 2020), https://techcrunch.com/2020/01/24/sonos-clarifies-how-unsupported-devices-will-be-treated/.
[15] 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/.
[16] Federal Trade Commission Public Comment on "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers" Communicating Upgradability and Improving Transparency Working Group Multistakeholder Process on Internet of Things Security Upgradability and Patching, National Telecommunications & Information Administration (2017), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.

Consumer Reports

cc: The Honorable Jacqui Irwin
Members, Assembly Privacy and Consumer Protection Committee