California State Senate
Senate Judiciary Committee
1021 O Street, Suite 3240
Sacramento, CA 95814

Re: Senate Bill 898: Support

Dear Members of the Senate's Judiciary Committee:

Consumer Reports strongly supports SB 898 which would provide transparency around how long consumers can expect their connected devices to operate in a safe and secure manner. The bill has an added benefit of improving national and personal security.

Consumers are purchasing more devices that connect to the internet in the form of smart TVs, smart home products and even large appliances. But over time connected products lose software support, which can affect their security and also their features. For example, a connected TV that loses support may not support certain apps or a router that no longer gets updates becomes a potential security risk.[1] Some devices may stop working altogether.

Consumers deserve to know how long their products will work

This is not something consumers are necessarily aware of. In December 2024, Consumer Reports conducted a nationally representative survey of 2,130 Americans that found that four in ten (43%) owners of a connected device said that the last time they purchased one they were not aware that it might lose software support at some point.[2]

The lack of awareness is unsurprising given that manufacturers don't necessarily publish this information or make it easy to find. The Federal Trade Commission researched 184 connected products only to discover that only 21 — or 11.4% — disclosed the device's software support

[1] Federal Bureau of Investigation. "Cyber Criminal Services Target End-of-Life Routers to Launch Attacks and Hide Their Activities." FBI Flash. Flash-20250507-001. May 7, 2025. https://www.ic3.gov/CSA/2025/250507.pdf

[2] S. Higginbotham. "Hey Siri, Are You a Zombie? Consumer Reports Innovation Blog." Feb. 5, 2025. https://innovation.consumerreports.org/hey-siri-are-you-a-zombie/

duration or end date on the product web page.[3] Consumer Reports surveyed 21 of the top large appliance brands and found that only three brands tell consumers how long they guarantee updates to their appliances' software and applications.[4] That same nationally representative survey from December 2024 also found that 72% of Americans who have purchased smart devices believe manufacturers should be required to disclose how long they will support those devices.[5]

This bill would help consumers to make informed purchases by requiring manufacturers to put a minimum guaranteed support time frame on product web pages, and disclose that time frame at the point of purchase. It also would require manufacturers to proactively let consumers know when a connected device loses support. These two simple provisions would greatly improve cybersecurity by ensuring consumers can more effectively choose and use supported devices, which in turn will greatly reduce the number of unsupported devices on the internet that are available for cyberattacks.

From a marketplace perspective, requiring all manufacturers to specify a minimum guaranteed support time frame creates a level playing field for competition, so that companies that disclose information on end of product life are not undercut by companies who don't. It also will likely push smart device manufacturers to compete on device longevity. We have seen this play out over the last decade in smartphones with stated software support time frames going from two or three years to seven years. That increase in support time frames boosted smartphone longevity, and reduced e-waste.[6]

A minimum guaranteed support time frame is incredibly useful for consumers purchasing connected devices, especially as these products are becoming more common, and more expensive, than their "dumb" counterparts. Research from Parks Associates indicates that consumer IoT products are priced 21% to 70% higher than similar non-connected products, with an average price differential of 44%.[7] Plus, by requiring companies to support a minimum guaranteed support time free, the law allows manufacturers to extend that time frame at their

---

[3] U.S. Federal Trade Commission. "Smart Device Makers' Failure to Provide Updates May Leave You Smarting." Nov. 2024
https://www.ftc.gov/reports/smart-device-makers-failure-provide-updates-may-leave-you-smarting

[4] S. Higginbotham. "When Will Your Smart Appliance Turn Dumb? A Lack of Transparency Leaves Consumers in the Dark." Consumer Reports Innovation Blog. Sept. 25, 2024.
https://innovation.consumerreports.org/when-will-your-smart-appliance-turn-dumb/

[5] N. Altman. "American Experiences Survey: December 2024 Omnibus Data" Consumer Reports Survey Research Department. Jan. 2025.
https://article.images.consumerreports.org/image/upload/v1736806650/prod/content/dam/surveys/Consumer_Reports_AES_December_2024.pdf

[6] Atrina Oraee, Lara Pohl, Daniëlle Geurts, Max Reichel,
Overcoming Premature Smartphone Obsolescence amongst Young Adults, Cleaner and Responsible Consumption, Volume 12, 2024, 100174, ISSN 2666-7843,
https://doi.org/10.1016/j.clrc.2024.100174.

[7] J. Kent, S. Jiang, Y. Mu. "The Business of Consumer IoT: Product Strategy in a Maturing Market." Parks Associates. June 2025.
https://www.parksassociates.com/products/home-controls-home-systems-home-automation-and-controls/the-business-of-consumer-iot-product-strategy-in-a-maturing-market

discretion. For example, Apple, Amazon, Signify (which makes Philips Hue products), and other manufacturers have published — and then subsequently extended — their support time frames for their connected products.

Competition around support times frames reduces e-waste

Providing this information gives consumers essential information about how long they can expect their products to work and remain secure, allowing them to select products that will receive support for longer periods of time. This should drive manufacturers to build longer-lived products, which in turn, will reduce the number of devices sent to landfills simply because they stopped getting necessary security updates.

Research from the U.S. Public Interest Research Group in April 2025 estimates that the loss of software support and cloud connectivity for connected devices has led to the creation of a minimum of 130 million pounds of electronic waste since 2014.[8] While we still expect companies who make connected devices to stop supporting them over time, this law would help drive manufacturers to compete on device longevity, educate consumers about the expected useful life of their connected products, and in turn should lead to longer life cycles for connected consumer devices.

As an additional incentive for manufacturers to offer high-quality devices, Consumer Reports also would like to see the bill require companies to ensure that their minimum guaranteed support time frames are commensurate with reasonable consumer expectations for the life of the product. For example, a consumer buying a connected GE oven can only expect software updates two years from the original purchase date or five years from the appliances' launch date, whichever is longer.[9] However consumers expect their large appliances to last an average of 12 years. Two in five Americans (38%) said a large appliance should reasonably last more than ten years. Another two in five (40%) said it should last exactly ten years.[10]

But if essential software features are only supported for up to five years, consumers buying a connected oven could lose those essential features midway through their expected life of the product.

Clear support time frames reduce cybersecurity risks

---

[8] L. Gutternan. "Electronic Waste Graveyard." U.S. PIRG. April 10, 2025. https://pirg.org/edfund/resources/electronic-waste-graveyard/

[9] S. Higginbotham. "When Will Your Smart Appliance Turn Dumb? A Lack of Transparency Leaves Consumers in the Dark." Consumer Reports Innovation Blog. Sept. 25, 2024. https://innovation.consumerreports.org/when-will-your-smart-appliance-turn-dumb/

[10] Consumer Reports. Right to Repair Survey: A Nationally Representative Multi-Mode Survey. August 2024. https://article.images.consumerreports.org/image/upload/v1723220409/prod/content/dam/surveys/Consumer_Reports_Right_to_Repair_June_July_2024.pdf

The bill would also help improve public and consumer cybersecurity. When consumers keep connected devices such as routers and IoT products online after they have stopped receiving software and security updates, it leaves these products open to cyberattack. We call these devices zombies. Attackers can also use the zombie devices to access home networks. But consumers have no way of knowing when their device becomes a zombie if the manufacturer doesn't tell them.

Zombie devices post a very real security risk, because they can easily get hacked and become part of botnets used to take down web sites and services, or be used to establish footholds in networks. Nation states and malicious actors have taken over routers and IoT products that have reached their end of life to launch botnets.[11]

In November 2025, a security researcher warned that thousands of end of life Asus routers, including thousands in the United States, have been taken over by Chinese hackers and are likely used for espionage.[12] In March the FBI issued a warning for consumers to stop using 20 routers — many of which were no longer receiving software updates — because they were actively being exploited by malware.[13] The FBI warned that hackers were leasing the botnet running on these end of life devices to criminals to conduct various types of fraud and coordinated attacks on web sites.

Consumer Reports supports Senate Bill 898, and believes it will provide consumer protections as connected devices become more common, allowing consumers to make informed decisions and reward companies that behave responsibly. It also should lead to longer-lived products that will help reduce e-waste while also boosting overall cybersecurity.

We would like the bill amended to add a requirement that the support period should match reasonable consumer expectations associated with the device, which augments the disclosure requirements with additional protections. We urge committee members to support SB 898.

Thank you for your time.

Stacey Higginbotham
Policy Fellow
Consumer Reports

---

[11] Trend Micro Research "IoT Botnet Linked to Large-scale DDoS Attacks Since the End of 2024." Jan. 17, 2025. https://www.trendmicro.com/en_us/research/25/a/iot-botnet-linked-to-ddos-attacks.html

[12] Security Scorecard Research. "Thousands of ASUS Routers Hijacked in Global Operation "WrtHug" in a Suspected China-Backed Campaign." November 2025. https://securityscorecard.com/wp-content/uploads/2025/11/STRIKE_Asus_WrtHug-Report_V6.pdf

[13] FBI. AVrecon Malware-Infected Routers Exploited as Residential Proxies by SocksEscort. FBI Flash. Flash No. 20260312-001. March 12, 2026. https://www.fbi.gov/investigate/cyber/alerts/2026/avrecon-malware-infected-routers-exploited-as-residential-proxies-by-socksescort