MEMORANDUM IN SUPPORT OF A.10132 and S.8507

SYNOPSIS: Enacts the "connected consumer product end of life disclosure act", relating to requiring manufacturers of connected consumer products to disclose for how long they will provide technical support, security updates, or bug fixes for the software, hardware, or firmware necessary for the product to securely function.

INTRODUCED BY: Senator Patricia Fahy and Assemblyman Steve Otis

STATEMENT OF SUPPORT: Consumer Reports strongly supports A.10132 and S.8507 which would improve national and personal security while also providing transparency around how long consumers can expect their connected devices to operate in a safe and secure manner.

More and more consumer products are connected to the internet. But 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.

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.[1]

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[2]. In May the FBI had to issue a warning for consumers to stop using 13 different routers because they were susceptible to malware and were no longer supported[3]. The FBI warned that hackers were leasing the botnet running on these end of life devices to criminals for coordinated attacks on web sites.

---

[1] 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

[2] 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

[3] 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

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.

Generally, consumers may be unaware that their connected products lose software support, which can affect their security and also their features. 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.[4]

This 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 duration or end date on the product web page.[5] 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.[6] That same nationally representative survey from Dec. 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.

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 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 zombie 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. Increasing software support does increase smartphone longevity, and reduces e-waste.[7]

---

[4] 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/

[5] 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

[6] 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/

[7] 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.

This information 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%.[8] Plus, by requiring companies to support a minimum guaranteed support time free, the law allows manufacturers to extend that time frame at their discretion. Apple, Amazon, Signify (which makes Philips Hue products) and other manufacturers have announced, and then extended their support time frames for their connected products.

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.[9] 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.

For all these reasons, Consumer Reports strongly urges you to vote YES for A.10132 and S.8507, to improve overall cybersecurity, inform consumers’about how long their connected products might last, and influence manufacturers to support their connected products for a longer period of time, reducing e-waste.

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