SENATE PRIVACY, DIGITAL TECHNOLOGIES, AND CONSUMER PROTECTION COMMITTEE
Senator Christopher Cabaldon, Chair
2025-2026 Regular Session

SB 898 (Weber Pierson)
Version: March 24, 2026
Hearing Date: April 13, 2026
Fiscal: Yes
Urgency: No
CK

SUBJECT

Connected consumer products

DIGEST

This bill requires manufacturers of connected consumer products to establish minimum guaranteed support timeframes for their products and to disclose support timeframes before purchase and as the product reaches its end of life.

EXECUTIVE SUMMARY

According to the National Institute of Standards and Technology (NIST):

> The Internet of Things has unlimited possibilities for home and business use. Appliances from refrigerators to sensor networks are now available in models that interact with a wireless network, making them easier to control with a computer or smartphone. Estimates suggest that there will be more than 75 billion IoT devices in use by 2025, according to IHS Markit.
>
> Along with this massive market adoption of IoT, though, comes a trove of security concerns that necessitate attention and action.[1]

The billions of connected devices have varied functionality and implemented various levels of security. Existing law requires connected devices to be equipped with reasonable security features that are appropriate for the device, as provided. However, concerns have arisen that such devices are widely in use around the world but that consumers are ill-prepared and uninformed when manufacturers no longer provide security updates and full functionality for these devices. This bill requires

[1] Security Guide, *Internet of Things (IoT)*, NIST, https://www.nccoe.nist.gov/iot. All internet citations are current as of April 7, 2026.

manufacturers of connected consumer products to disclose to consumers a minimum guaranteed support timeframe and to notify consumers as the product is reaching its end of life. Those businesses leasing or providing customers with such products must ensure the products are updated promptly and replaced when no longer supported.

This bill is author sponsored. It is supported by Consumer Reports and CALPIRG. No timely opposition was received by the Committee. Should the bill pass out of this Committee, it will next be heard by the Senate Judiciary Committee.

PROPOSED CHANGES TO THE LAW

Existing law:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, Sec. 1.)

2) Requires a manufacturer of a connected device to equip the device with a reasonable security feature or features that are all of the following:
    a) Appropriate to the nature and function of the device.
    b) Appropriate to the information it may collect, contain, or transmit.
    c) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure. (Civ. Code § 1798.91.04(a).)

3) Provides that subject to all of the above requirements, if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature if the preprogrammed password is unique to each device manufactured or the device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time. (Civ. Code § 1798.91.04(b).)

4) Defines "connected device" as any device or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address. (Civ. Code § 1798.91.05.)

5) Provides a series of clarifying exemptions and limitations to the above provisions. (Civ. Code § 1798.91.06.)

6) Requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure and requires such businesses to contractually require nonaffiliated

third parties to which it discloses such personal information to similarly protect that information. (Civ. Code § 1798.81.5(b), (c).)

7) Establishes the California Consumer Privacy Act (CCPA), which grants consumers certain rights with regard to their personal information, including enhanced notice, access, and disclosure; the right to deletion; the right to restrict the sale of information; and protection from discrimination for exercising these rights. It places attendant obligations on businesses to respect those rights. (Civ. Code § 1798.100 et seq.)

8) Establishes the Unfair Competition Law (UCL), which provides a statutory cause of action for any unlawful, unfair, or fraudulent business act or practice and unfair, deceptive, untrue, or misleading advertising, including over the internet. (Bus. & Prof. Code § 17200 et seq.)

9) Requires actions for relief pursuant to the UCL be prosecuted exclusively in a court of competent jurisdiction and only by the following:
    a) the Attorney General;
    b) a district attorney;
    c) a county counsel authorized by agreement with the district attorney in actions involving violation of a county ordinance;
    d) a city attorney of a city having a population in excess of 750,000;
    e) a county counsel of any county within which a city has a population in excess of 750,000;
    f) a city attorney in a city and county;
    g) a city prosecutor in a city having a full-time city prosecutor in the name of the people of the State of California upon their own complaint or upon the complaint of a board, officer, person, corporation, or association with the consent of the district attorney; or
    h) a person who has suffered injury in fact and has lost money or property as a result of the unfair competition. (Bus. & Prof. Code § 17204.)

10) Establishes the Song-Beverly Consumer Warranty Act, which sets forth standards for warranties that govern consumer goods and outlines remedies available to purchasers. The Act requires every sale of consumer goods that are sold at retail in this state to be accompanied by the manufacturer's and the retail seller's implied warranty that the goods are merchantable. (Civ. Code § 1790 et seq.)

This bill:

1) Requires a manufacturer to clearly and prominently establish and disclose to any prospective buyer of a connected consumer product a minimum guaranteed support timeframe in both of the following ways:

a) At the point of sale, if practicable.
b) In a clear and conspicuous manner on the product packaging and on the manufacturer's website or product-specific webpage.

2) Prohibits a manufacturer from reducing that minimum guaranteed support timeframe.

3) Requires a manufacturer to provide a notice of a connected consumer product's end of life to the public and to any owner of the product six months before the product reaches end of life and the date on which the product reaches end of life.

4) Provides that the above notification shall include clear information about any action a consumer can take if the consumer wants to continue using the connected consumer product in a secure and effective manner and provide a list of features lost, security risks, reduced interoperability, or any other changes that are likely to result from the connected consumer product's end of life.

5) Requires a business that owns or controls a connected consumer product that it leases or otherwise provides to its customers as part of a service to do both of the following:
   a) Ensure that updates provided by the manufacturer for the connected consumer product are promptly received and applied.
   b) When the connected consumer product has reached its end of life, replace the connected consumer product, at no additional cost to the customer, with a comparable product capable of receiving necessary updates and support if a comparable product is reasonably available to the business.

6) Deems a violation a deceptive act or practice under the UCL.

7) Defines the relevant terms:
   a) "Connected consumer product" means a product, including a physical device, mobile application, or any necessary cloud infrastructure, that is intended for consumer use and is capable of connecting to the internet, either directly or indirectly.
   b) "End of life" means the point after which the manufacturer no longer provides necessary support or updates for a connected consumer product.
   c) "Manufacturer" means the manufacturer of a connected consumer product sold at retail in the state.
   d) "Minimum guaranteed support timeframe" means the minimum amount of time for which a company commits to providing all necessary updates and support to a connected consumer product that includes a specific date at the end of the timeframe.

COMMENTS

1. Understanding the risks posed by connected products at their end of life

As stated, existing law requires connected devices to be equipped with reasonable security features that are appropriate for the device, as provided. "Connected devices" are defined as any device or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address. Recent legislation created a safe harbor within that statute that encourages manufacturers to meet baseline standards established by NIST in response to an executive order issued by President Biden. A manufacturer is deemed in compliance with the statute if the connected device meets or exceeds the NIST baseline criteria.

Serious concerns arise when manufacturers of these products stop supporting them and security updates are no longer taking place. Most consumers are unaware of when this occurs and open themselves up to serious security risks. This is not a new issue, as the Federal Trade Commission (FTC) flagged the issue almost a decade ago:

> The Internet of Things refers to consumer products that connect to the Internet to send and receive data – everything from fitness devices, wearables, and smart cars to connected smoke detectors, light bulbs, and refrigerators. These new products bring enormous benefits to consumers – including the ability to track and share their vital signs with care providers without having to go to a doctor's office, turn off the burglar alarm and turn on the lights before they get home from work, and even notify them of dangerous road conditions while driving a smart car.
>
> But what happens when the "things" can no longer connect to the Internet, or there are no longer updates or support for the "things"? A recent FTC investigation into one company's decision to stop providing support for an IoT device illuminates some pitfalls IoT businesses should avoid in introducing and marketing these innovative products. In that case, a company acquired the marketer of a "Smart Home Hub" and then decided to shut down support for the device, thereby rendering it inoperable. Although we closed that investigation, it raises broader issues about what happens when an IoT product or service, or the updates and support for them, stops.
>
> First, there are serious issues at play when consumers purchase products that unexpectedly stop functioning due to a unilateral decision by the company that sold it. Consumers generally expect that the things they buy will work and keep working, and that includes any technical or other support necessary for essential functioning.

> Second, when a company stops providing technical support, including security updates, for an IoT device, consumers may be left with an out-of-date product that is vulnerable to critical security or privacy bugs. This could create vulnerabilities for other systems connected to these IoT devices, and put consumers' sensitive data at risk. And if hackers can hack a smart car, pacemaker, or insulin pump, the risks are even more serious. We've previously raised these concerns in our report on the Internet of Things.[2]

However, with the tens of billions of connected products now in use across the world, national consumer groups and cybersecurity-focused organizations have sounded the alarm that something needs to be done:

> The proliferation of IoT devices in homes and businesses has created a significant security challenge. When these devices reach their end of life and no longer receive software and security updates, they become vulnerable to exploitation by malicious actors. These "zombie devices" can be hijacked and used in botnets, posing a risk to individual users and the wider internet.
>
> "Consumers deserve to know how long their connected devices will be supported," said Justin Brookman, director of technology policy for Consumer Reports. "Currently, it's nearly impossible for most people to figure out if their devices are still receiving critical updates. This lack of transparency leaves consumers vulnerable and creates significant security risks."[3]

The risks are not trivial. The Cybersecurity and Infrastructure Security Agency (CISA), hailed as "America's Cyber Defense Agency," has also stressed the imminent threat such unsupported devices represent:

> The United States faces persistent cyber campaigns that threaten both public and private sectors, directly impacting the security and privacy of the American people. These campaigns are often enabled by unsupported devices that physically reside on the edge of an organization's network

---

[2] Jessica Rich, *What happens when the sun sets on a smart product?* (July 13, 2016) FTC, https://www.ftc.gov/business-guidance/blog/2016/07/what-happens-when-sun-sets-smart-product.

[3] Press release, *Consumer Reports, US PIRG, Secure Resilient Future Foundation, and the Center for Democracy and Technology Propose, "Connected Consumer Products End of Life Disclosure Act" to Address IoT Security Risks* (March 12, 2025) Consumer Reports, https://advocacy.consumerreports.org/press_release/consumer-reports-us-pirg-and-secure-resilient-future-foundation-propose-connected-consumer-products-end-of-life-disclosure-act-to-address-iot-security-risks/.

> perimeter. Unsupported devices – referred to in this Directive as "end of support (EOS)" – are those that are no longer maintained by their vendors.
>
> The imminent threat of exploitation to agency information systems running EOS edge devices is substantial and constant, resulting in a significant threat to federal property. CISA is aware of widespread exploitation campaigns by advanced threat actors targeting EOS edge devices. Recent public reports of campaigns targeting certain vendors highlight actors' attempts to use these devices as a means to pivot into [Federal Civilian Executive Branch] information system networks. Edge devices are attractive targets due to their extensive reach into an organization's network and integrations with identity management systems. These devices are especially vulnerable to cyber exploits targeting newly discovered, unpatched vulnerabilities. Additionally, they no longer receive supported updates from the original equipment manufacturer, exposing federal systems to disproportionate and unacceptable risks.[4]

One incident specifically involved attacks by a foreign government on routers that had reached their end of life and were not being updated or supported by the manufacturer:

> A December 2023 court-authorized operation has disrupted a botnet of hundreds of U.S.-based small office/home office (SOHO) routers hijacked by People's Republic of China (PRC) state-sponsored hackers.
>
> The hackers, known to the private sector as "Volt Typhoon," used privately-owned SOHO routers infected with the "KV Botnet" malware to conceal the PRC origin of further hacking activities directed against U.S. and other foreign victims. …
>
> The vast majority of routers that comprised the KV Botnet were Cisco and NetGear routers that were **vulnerable because they had reached "end of life" status; that is, they were no longer supported through their manufacturer's security patches or other software updates**. The court-authorized operation deleted the KV Botnet malware from the routers and took additional steps to sever their connection to the botnet, such as blocking communications with other devices used to control the botnet.[5]

---

[4] Binding Operational Directive, *BOD 26-02: Mitigating Risk From End-of-Support Edge Devices* (February 5, 2026) CISA, https://www.cisa.gov/news-events/directives/bod-26-02-mitigating-risk-end-support-edge-devices.

[5] Press release, *U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure* (January 31, 2024) United States Department of Justice, https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical?bm-verify=AAQAAAAN____3v-

2. Addressing the risks posed by connected products

Given these critical risks, this bill places several obligations on manufacturers of "connected consumer products," defined as a product, including a physical device, mobile application, or any necessary cloud infrastructure, that is intended for consumer use and is capable of connecting to the internet, either directly or indirectly.

First, the bill requires manufacturers to establish a "minimum guaranteed support timeframe," defined as the minimum amount of time for which a company commits to providing all necessary updates and support to a connected consumer product that includes a specific date at the end of the timeframe. They must disclose this timeframe to prospective buyers both at the point of sale, if practicable, and in a clear and conspicuous manner on the product packaging and on the manufacturer's website or product-specific webpage. This support timeframe cannot be reduced.

Next, manufacturers must also provide a notice to the public and to any owner of the product six months before the product reaches end of life and the date upon which the product reaches end of life. "End of life" means the point after which the manufacturer no longer provides necessary support or updates for a connected consumer product. In order to ensure that these notices are clear and not buried with other information, the author has agreed to an amendment that requires them to be standalone notices.

Finally, the bill requires a business that owns or controls a connected consumer product that it leases or otherwise provides to its customers as part of a service to do both of the following:

- Ensure that updates provided by the manufacturer for the connected consumer product are promptly received and applied.
- When the connected consumer product has reached its end of life, replace the connected consumer product, at no additional cost to the customer, with a comparable product capable of receiving necessary updates and support if a comparable product is reasonably available to the business.

This latter provision is intended to address those situations where a consumer does not directly purchase the product and therefore puts the responsibility on businesses that are leasing or providing such products. Consumers rely on the functionality and software of leased products just as they do for products they own.

Vxqz6cdmn9qd_pbx6toCozEQ3oSj2OlhBOTZ2dv7aaduggJVIzZbRwH9nfEo52gkkulO5JtBK_zMB-KFWmUuWKbg-kD_OR4h8pvLYUPBiLtoW39boJtFdq6Ee401ipmEXojnWWK-2z1qQ4tiE78qJSiq05Lb9-ZIvPI8_uxwSQdMe-6K6bPNzTKYQ909ZElKDv0NbKbh2n7EJcwtB5ogYvb4QN9HWE_UDm8ltTtAbncKO3iYeH-QrLv1g3TYhQrnahzr_Is6maofe2BUQtyx-OHz5lgP_RNHQIOC9RqpOS9OcInIIRG1735J9kMh4hbDnzPSeh9RFs3Erw6YKPvOBdkgiUYZs0RfGISmhFyeiVCErjCiDkODSSCNfJW12MJFRGUoZE1oAww7oCXyiF2DoFCtYVWLrMYbLslMogIZu2f3nW2nXvnq4wTSTGiziXewgxCsJ88AZKI8.

Any violations are deemed deceptive acts or practices pursuant to the UCL.

According to the author:

> Connected "smart" products have become increasingly common in households across California, many of which rely on ongoing software updates to receive all necessary support. Consumers should know in advance and on the date when a manufacturer ultimately stops providing these critical updates, as their products may lose promoted or integral features, become vulnerable to security risks, or stop working altogether.
>
> A manufacturer's failure to clearly disclose the duration of their software support commitments warrants action. Current law does not require this transparency, leaving consumers without essential information about the products they have invested in. Research from the Federal Trade Commission found that nearly 90 percent of manufacturers of common connected products failed to disclose how long those devices would receive software updates or support on their product's webpages. Even when information is available, it is often not clearly provided at the point of sale or consistently and easily accessible before and after purchase.
>
> SB 898 establishes a clear transparency framework to advance consumer education. By requiring manufacturers to disclose a minimum guaranteed support time frame and provide notice when a product reaches its end of life, this bill ensures that consumers can make fully informed purchasing and operational decisions about the products they rely on every day.

This bill largely aligns with legislation that is also currently pending in the Massachusetts and New York legislatures, as well as regulations in the European Union. One issue that has been raised is that there is no floor for the minimum guaranteed support timeframe, so manufacturers can establish a de minimis timeframe. For reference, the bills currently pending in the New York Assembly and Senate both have the following provision: "The minimum guaranteed support time frame shall not be inconsistent with reasonable consumer expectations about how long a connected consumer product's features that depend upon internet connectivity should last." Similarly, the EU also incorporates "reasonable user expectations" regarding the support timeframe:

> For the purpose of ensuring the security of products with digital elements after their placing on the market, manufacturers should determine the support period, which should reflect the time the product with digital elements is expected to be in use. In determining a support period, a manufacturer should take into account in particular reasonable user

> expectations, the nature of the product, as well as relevant Union law determining the lifetime of products with digital elements. …
>
> The support period for which the manufacturer ensures the effective handling of vulnerabilities should be no less than five years, unless the lifetime of the product with digital elements is less than five years, in which case the manufacturer should ensure the vulnerability handling for that lifetime. Where the time the product with digital elements is reasonably expected to be in use is longer than five years, as is often the case for hardware components such as motherboards or microprocessors, network devices such as routers, modems or switches, as well as software, such as operating systems or video-editing tools, manufacturers should accordingly ensure longer support periods.[6]

To establish a floor for the minimum guaranteed support timeframe, the author has agreed to an amendment that requires the timeframe to be no less than five years.

In addition, some questions have arisen about the scope of the definition of "connected consumer product," as it currently applies not only to physical products but also mobile applications and "necessary cloud infrastructure." The author has committed to working with the Committee on refining this definition.

3. Stakeholder positions

Consumer Reports writes in support:

> 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. 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.
>
> 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

[6] Regulation (EU) 2024/2847 of the European Parliament and of the Council, Paragraphs 59-60 (October 23, 2024) European Union, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202402847.

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.

SUPPORT

CALPIRG
Consumer Reports

OPPOSITION

None received

RELATED LEGISLATION

AB 1921 (Ward, 2026) requires operators of digital games to provide specified information to purchasers and prospective purchasers at least 60 days before a digital game operator ceases to provide services necessary for the ordinary use of the digital game, including the date of cessation and information about lost features and services and any known security risks. AB 1921 is currently in the Assembly Privacy and Consumer Protection Committee.

SB 50 (Ashby, Ch. 676, Stats. 2025) requires account managers of connected devices to provide a process for survivors or their representatives to terminate or disable perpetrators' access to such devices through a "device protection request" with specified documentation from survivors of "covered acts," as defined.

AB 2392 (Irwin, Ch. 785, Stats. 2022) provides that manufacturers of connected devices satisfy existing security requirements regarding connected devices by meeting certain baseline labeling standards established by NIST.

SB 327 (Jackson, Ch. 886, Stats. 2018) requires manufacturers of connected devices to equip those devices with reasonable security features appropriate to the nature of the device.

****