Date of Hearing: June 30, 2026

ASSEMBLY COMMITTEE ON JUDICIARY
Ash Kalra, Chair
SB 898 (Weber Pierson) – As Amended June 25, 2026

SENATE VOTE: 30-8

SUBJECT: CONNECTED CONSUMER PRODUCTS

SYNOPSIS

The "Internet of Things" (IoT) refers to the growing ecosystem of internet-connected devices—thermostats, smart locks, lights, speakers, cameras, and appliances—that collect and exchange data with users and each other. These technologies offer convenience, but rely on software support from the manufacturer, or third-party. As internet-connected devices become embedded in homes, cars, and personal belongings, consumers should have clear expectations about the duration of software support they will receive for their purchases. This bill requires manufacturers to clearly disclose the minimum amount of time consumers can rely on their connected product to receive necessary updates and support. Additionally, it requires advanced and day-of notice of the product's "end of life" (EOL) date, when these updates and support will definitively no longer be provided.

This bill is supported by Consumer Reports and other consumer protection organizations. The bill is opposed by the Alliance for Automotive Innovation, the Consumer Technology Association, and several business- and industry-aligned advocacy groups. The bill passed out of the Assembly Committee on Privacy and Consumer Protection by a vote of 11-4.

SUMMARY: 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. Specifically, **this bill**:

1) Requires a manufacturer to clearly and conspicuously disclose a connected consumer product's minimum guaranteed support timeframe to any prospective buyer of the product, as provided.

2) Prohibits a manufacturer from reducing a minimum guaranteed support timeframe that has been disclosed to a prospective buyer, unless the manufacturer demonstrates that providing support for the connected consumer product is not feasible due to unforeseeable circumstances beyond the manufacturer's reasonable control, including any of the following:

    a) The manufacturer is subject to bankruptcy or another insolvency proceeding that materially impairs the manufacturer's ability to provide support;

    b) A third-party dependency, including, but not limited to, a service, platform, software or hardware component, security certificate, application programming interface, network, or other technology operated or controlled by an unaffiliated third party that is necessary to provide support, is discontinued, materially altered, or no longer made available to the manufacturer on commercially reasonable terms and cannot reasonably be replaced by the manufacturer;

c) Providing support is unlawful; or

d) A vulnerability, defect, or other safety or security condition makes providing support materially likely to compromise the security, privacy, or safety of users or the public, and the issue cannot reasonably be remedied by the manufacturer.

3) Requires that a minimum guaranteed support timeframe established by a manufacturer is consistent with the reasonable expectations of a consumer based on the following:

a) The nature of the connected consumer product, including the connected consumer product's expected use, durability, and reliance on remote services;

b) The price paid for the connected consumer product by consumers;

c) How the connected consumer product is advertised, marketed, or otherwise described by the manufacturer at the time of purchase; and

d) The minimum guaranteed support timeframe of comparable connected consumer products.

4) Requires a manufacturer to provide notice to the public and any owner of a connected consumer product both six months before and upon the connected consumer product reaching its end of life. The notice is required to contain information about any action the owner can take to continue using the product in a secure and effective manner, as well as a list of product features lost, security risks, and other changes due to the product reaching end of life. Requires that the notice be a standalone communication containing no other information.

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, the extent technically feasible, ensure that security patches made available by the manufacturer are promptly applied, and if the connected consumer product reaches its end of life, to notify the customer and replace the product with a comparable connected consumer product that has not reached end of life, if one is reasonably available to the business.

6) Provides that a violation of the chapter constitutes a deceptive act or practice under the Unfair Competition Law (UCL).

7) Defines the following terms:

a) "Connected consumer product" means a physical product, including a mobile application or cloud infrastructure related to the functioning of the physical product, that is intended for consumer use and depends on a connection to the internet for a consumer to make ordinary use of the product.

b) "End of life" means the date on which a manufacturer no longer provides support, security patches, or updates that are necessary for a consumer to make ordinary use of 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 period of time, beginning when a manufacturer first makes a connected consumer product available for purchase in this state and ending on a specific date, during which a manufacturer commits to providing all necessary support, security patches, or updates that are necessary for a consumer to make ordinary use of a connected consumer product.

e) "Ordinary use" means use of a connected consumer product that is consistent with a consumer's reasonable expectations based on how the connected consumer product was advertised, marketed, or otherwise described by the manufacturer at the time of purchase.

EXISTING LAW:

1) Establishes the UCL, which provides a statutory cause of action for any unlawful, unfair, or fraudulent business act or practice and any unfair, deceptive, untrue, or misleading advertising, including over the internet. (Business and Professions Code Section 17200 *et seq*.)

2) Requires actions for relief pursuant to the UCL be prosecuted exclusively in a court of competent jurisdiction and only by any of the following:

   a) The Attorney General;

   b) A district attorney;

   c) A county counsel authorized by agreement with the district attorney in actions involving a 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 act of unfair competition. (Business and Professions Code Section 17204.)

3) Provides that it is unlawful for any person doing business and advertising in this state to make any false or misleading advertising claim. (Business and Professions Code Section 17508.)

4) Requires every sale of consumer goods 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. (Civil Code Section 1792.)

5) 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; and

   c) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure. (Civil Code Section 1798.91.04 (a).)

6) Provides that, subject to the requirements in 5), 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. (Civil Code Section 1798.91.04 (b).)

7) 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, subject to specified exemptions and limitations. (Civil Code Sections 1798.91.05, 1798.06.)

8) 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. (Civil Code Section 1798.81.5 (b), (c).)

9) 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. (Civil Code Section 1798.100 *et seq*.)

FISCAL EFFECT: As currently in print this bill is keyed fiscal.

COMMENTS: The "Internet of Things" (IoT) refers to the growing ecosystem of internet-connected devices—thermostats, smart locks, lights, speakers, cameras, and appliances—that collect and exchange data with users and each other. These technologies offer convenience, but rely on software support from the manufacturer, or third-party. As internet-connected devices become embedded in homes, cars, and personal belongings, consumers should have clear expectations about the duration of software support they will receive for their purchases. 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.

Connected smart devices are increasingly present in the home and elsewhere. The role of connected devices, or devices that can connect to the internet and have an Internet Protocol or Bluetooth Address, in the daily lives of Americans has skyrocketed in recent years with the emergence of smart technologies designed to increase personal comfort, convenience, and efficiency. (*See* Civil Code Section 1798.91.05 (b).) These devices are varied in nature, and include Wi-Fi enabled thermostats, speakers, door locks, cameras, lights, security systems, sprinklers, and refrigerators, all of which can be operated remotely from smartphone apps, computer programs, or internet websites.

According to a 2024 Consumer Reports survey, only 35% of consumers were aware that these connected products could lose software support at some point. (*American Experiences Survey: A Nationally Representative Multi-Mode Survey* (Dec. 2024) Consumer Reports, pg. 12, available at: https://article.images.consumerreports.org/image/upload/v1736806650/prod/content/dam/surveys/Consumer_Reports_AES_December_2024.pdf.) A Federal Trade Commission (FTC) Staff Report surveyed the websites of 184 connected products and found that almost 90 percent of these web pages did not disclose how long the products would receive software updates. (*FTC Staff Report: Smart Device Makers' Failure to Provide Updates May Leave You Smarting* (Nov. 2024) FTC Bureau of Consumer Protection available at: https://www.ftc.gov/system/files/ftc_gov/pdf/smart-device-makers-failure-to-provide-software-updates-may-leave-you-smarting.pdf.) These devices may not function fully without software support and, according to the author, they may be more susceptible to ransomware attacks without regular security updates.

This bill requires manufacturers of connected consumer products to set minimum guaranteed support timeframes for connected consumer products, based on the reasonable expectations of a consumer. The bill specifies the factors to consider in establishing what the consumer's reasonable expectation would be, such as the nature of the product and the price paid. Generally, a manufacturer may not shorten this support timeframe, however, the bill provides an exception if the support timeframe is no longer feasible due to unforeseen circumstances. These unforeseen circumstances could include the manufacturer is subject to bankruptcy, continuing support would likely lead to compromising user privacy, or the product relied on a third-party service or application for connectivity, and the third-party service or application is no longer available.

In addition to requiring a guaranteed minimum support timeframe, the bill requires manufacturers to make certain disclosures and notices regarding the support timeframe. First, the manufacturer must disclose the timeframe to prospective buyers, including on the product's packaging and the manufacturer's website. If the manufacturer reduces the support timeframe, due to circumstances discussed above, then they must notify any affected customer. Lastly, the date a product reaches its end of life, and six months prior, the manufacturer must notify the public and any product owners. The notification must include information on how to keep using the product (if applicable), and a list of the features lost and potential security risks. This notification is required to be sent via the product's interface (if practicable), to an owner's email (if the manufacturer knows their email), and placed on the manufacturer's website (for the public).

For businesses that may own connected consumer products that are then leased or provided to customers as part of a service, the bill requires these businesses to ensure that security patches made available for these products are promptly applied. Upon the end of life of a leased connected consumer product, the business must notify the customer and replace the product, at no additional cost, with a comparable connected product that has not reached its end of life, if one is reasonably available. For example, if a customer has leased a connected product—like a robot vacuum cleaner—where the product's functionality relies on its connection to the internet or Bluetooth, and the vacuum reaches its end of life, the business would need to replace the customer's vacuum with a functioning one, at no cost to the customer.

The bill provides that any violation of the bill constitutes a deceptive act or practice under the UCL. The UCL protects consumers against unlawful, unfair, or fraudulent business practices and advertising. The UCL provides remedies for "anything that can properly be called a business practice and that at the same time is forbidden by law." (*Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 180 [citations omitted].) The UCL provides for civil penalties to be assessed and recovered from violators in the name of the people of California by various governmental agencies and specifically details how the proceeds from those actions are to be distributed and used.

***Commercial Speech*.** The First Amendment provides that "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." (U.S. Const., amend. I.) While commercial speech is a type of content-based restriction, and content-based restrictions ordinarily receive strict scrutiny analysis under the First Amendment, the U.S. Supreme Court has held that the First Amendment accords commercial speech lesser protection than other constitutionally guaranteed expression. This is in part because, unlike other varieties of speech, speech proposing a commercial transaction occurs in an area traditionally subject to *governmental regulation.* (*Central Hudson Gas & Elec. Corp. v. Public Service Commission* (1980) 447 U.S. 557, 562-63.) Ultimately, the First Amendment prohibits commercial speech against "unwarranted" governmental regulation.

The U.S. Supreme Court has articulated a four-prong test by which commercial speech regulations are evaluated for constitutionality. This test asks: (1) whether the expression concerns lawful activity and is not misleading; (2) whether the asserted governmental interest is substantial; (3) whether the regulation directly advances the governmental interest asserted; and

(4) whether it is not more extensive than is necessary to achieve that interest. (*Central Hudson Gas & Elec. Corp*., *supra*, 447 U.S. at pp. 561-66.)

For the first prong, the expression concerns a lawful activity, in this case a disclosure of the support timeframe of a product, and is not misleading, since it is providing the consumer with reasonable expectations for support of the product. The government interest, making sure that consumers reasonably understand the timeframe of functionality of a product so that they may spend their money wisely, appears to be a substantial one. The government does not want individuals to spend money on products that will not last very long, which can lead to negative economic repercussions. The regulation asserted that manufacturers clearly state the products support timeframe and notify when the timeframe is coming to an end, advances the government's interest of protecting consumers. The bill requires disclosures of a product's support timeframe, limitation of features after the end of life, and potential security risks. This would seem to be narrowly tailored to just the specific information needed for consumers to make informed decisions. Therefore, there are likely no First Amendment issues with the bill.

Additional considerations. The author has already substantially amended the bill since introduced to assuage many of the opposition's concerns and provide clarity to the bill's definitions and requirements. The following are some additional considerations for the author. First, as the bill is in print, a connected consumer product is one that requires an internet connection to make ordinary use of the product. Ordinary use is use that is consistent with a consumer's reasonable expectations based on how the product was advertised, marketed, or otherwise described by the manufacturer. These definitions appear to adequately capture the group of products the bill is attempting to regulate. That being said, some products, like automobiles that have an internet interface built in, may fall under this umbrella, which the author may not intend. *The author may wish to consider including language that specifies connected consumer products are those where the "primary purpose" or the "core functionality" of the product relies on internet connectivity.*

Although creating a laundry list of exempted products in the bill would likely be cumbersome and could potentially weaken the bill, there may be specific products that require such an exemption. For example, products that are used for medical or health care purposes or recommended by health care providers, and that are sold over the counter to consumers. By including these products under the bill's requirements, it may create unforeseen consequences for medical suppliers and products, and in turn, patients. *If the author wishes to exclude products that are predominantly used in a health care setting or prescribed by a health care provider, they may wish to include language to exclude these products from the bill's requirements.*

The bill has been amended to allow manufacturers to shorten the support timeframe due to several unforeseen circumstances. One of those is if a third-party dependency, such as a service or application, provides the connectivity to the product, and that third-party dependency ceases to operate, then the manufacturer may shorten the support timeframe. Although this provides manufacturers with some flexibility, it may still lead to difficulty adhering to some of the bill's requirements, such as the six-month notice before the end of life of a product. *If the author wishes to provide broader liability protection to manufacturers when a third-party dependency is at issue, they may consider language such as:*

A manufacturer is not liable for a failure to comply with this chapter that resulted from the act or omission of a third-party dependency not controlled by the manufacturer, if the manufacturer made commercially reasonable efforts to comply.

***ARGUMENTS IN SUPPORT**:* This bill is supported by Consumer Reports and other consumer protection organizations. Consumer Reports write in support:

> 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. Some devices may stop working altogether.
>
> […]
>
> 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.

The Secure Resilient Future Foundation (SRFF) writes in support:

> SB 898 requires the manufacturers of Internet-connected consumer products to disclose to consumers before they purchase a device the period of time they intend to provide technical support for the software that powers the device, including software updates, security patches and fixes for software bugs needed to keep the software and hardware secure and functioning properly.
>
> As a nonprofit organization representing cyber security- and information technology professionals, SRFF supports SB 898 because it addresses a dire security risk facing California’s families, businesses, communities: cybercriminal and state-backed hacking groups that exploit abandoned, vulnerable and un-patchable devices to launch disruptive cyber attacks.
>
> […]
>
> **End of life devices pose a cyber risk**

These attacks are possible because connected, “smart” devices that have been declared “end of life” or “end of support” by their manufacturers continue to maintain their connections to the Internet, but stop receiving needed software updates and security patches. These abandoned devices – broadband routers, security cameras, smart doorbells and kitchen appliances – are fodder for cybercriminal and nation-backed hacking crews that exploit known, but unpatched security flaws.

For example, researchers at Lumen Technology’s Black Lotus Lab wrote in March, 2024 about “Faceless,” a botnet consisting of tens of thousands of compromised end of life (EoL) smart home devices such as broadband routers that was “an integral tool for cybercriminals in obfuscating their activity.”

***ARGUMENTS IN OPPOSITION**:* The bill is opposed by the Alliance for Automotive Innovation, the Consumer Technology Association, and several business- and industry-aligned advocacy groups. The Alliance for Automotive Innovation writes in opposition, unless amended:

While a guaranteed support timeframe and an "end-of-life" replacement mandate may be suited for some types of consumer electronics, applying these same standards to motor vehicles creates infeasible legal, commercial, and logistical conflicts. We ask you to consider the following unique dynamics of the automotive industry:

1. **The Complexity of Motor Vehicles and Third-Party Dependencies.** Modern vehicles are highly complex machines that often rely on interconnected modules and/or third-party cellular infrastructure (such as 4G or 5G networks) to provide telematics and connected services. Automakers are unable to control the servicing and overall lifespan of these telematics networks. For example, if a major cellular provider makes the decision to sunset a network, a vehicle's connected features may reach "end of life" through no fault of the manufacturer.

2. **Impacts on Auto Leasing (Section 22928.11(e)(2)).** Another concern lies in the leasing provisions of the bill. Section 22928.11(e)(2) requires a business that leases a connected product to replace it at no additional cost to the customer when it reaches its end of life. Applied to the auto industry, this could be interpreted to mean that if a specific connected module reaches its end of life during the term of a vehicle lease, the entire vehicle could be subject to replacement at no cost. This mandate is impractical as applied to vehicle leases, and would be commercially impossible for automakers to implement while continuing to sustain a healthy vehicle lease environment.

Automobile manufacturers already support the maintenance of vehicle hardware and software far beyond the lifespans of most consumer electronic products. Additionally, new vehicles already come with an express written warranty, which customers are well-accustomed to utilizing to address issues that may arise during the period of vehicle ownership.

The Civil Justice Association of California (CJAC) writes in opposition, unless amended:

CJAC's primary concern is SB 898's enforcement mechanism. By deeming any violation a deceptive act or practice under the UCL, the bill exposes manufacturers to sweeping litigation risk that is poorly calibrated to the bill's consumer protection goals. The UCL's

notably broad and at times vague application can leave companies exposed to liability even when they have made good-faith efforts to comply. This lack of clarity creates significant uncertainty for businesses attempting to understand and meet their obligations under SB 898.

Compounding this problem, the UCL does not require proof of intent. Companies may therefore face liability for inadvertent or technical violations regardless of whether there was any intent to mislead consumers. Under the UCL, claims may be brought not only by public prosecutors but also by private plaintiffs who can demonstrate injury in fact and a loss of money or property, and class actions are commonly brought on this basis. This creates a pathway for large-scale, attorney-driven litigation based on alleged technical violations rather than demonstrable consumer harm, even though SB 898 does not establish an express private right of action.

REGISTERED SUPPORT / OPPOSITION:

Support

CALPIRG, California Public Interest Research Group
Consumer Reports
Consumer Reports Advocacy
FULU Foundation
Ifixit
Secure Resilient Future Foundation INC.
Software Freedom Conservancy
The Repair Association

Support If Amended

Center for Democracy and Technology

Opposition

Association of Home Appliance Manufacturers
Consumer Technology Association

Oppose Unless Amended

Advanced Medical Technology Association (ADVAMED)
Alliance for Automotive Innovation
Association of Home Appliance Manufacturers
California Chamber of Commerce
Civil Justice Association of California (CJAC)
Computer & Communications Industry Association
Entertainment Software Association
Ford Motor Company
General Motors
Technet
Toyota

Analysis Prepared by: Griff Ryan-Roberts / JUD. / (916) 319-2334