Date of Hearing: June 23, 2026

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 898 (Weber Pierson) – As Amended June 15, 2026

PROPOSED AMENDMENTS

SENATE VOTE: 30-8
SUBJECT: Connected consumer products

SYNOPSIS

Consumer products increasingly depend on internet connectivity to function as advertised. When manufacturers stop supporting these "connected consumer products," a device may lose key features, become vulnerable to cybersecurity threats, or stop working altogether even though the physical product remains intact. Existing law requires connected devices to include reasonable security features, but it does not require manufacturers to tell consumers how long those devices will receive the updates, patches, and support needed to remain safe and usable.

SB 898 creates a transparency and accountability framework for connected consumer products, requiring manufacturers of these products to clearly disclose their minimum guaranteed support timeframes at the point of purchase, provide notice before and when a product reaches end of life, and continue support consistent with reasonable consumer expectations based on the product's nature, price, marketing, and comparable products. This bill also requires businesses that lease or provide connected products as part of a service to apply security patches and replace unsupported products. Committee amendments would grant manufacturers more flexibility to set and adjust minimum support timeframes as appropriate, slightly narrow the scope of the bill by tying the definition of "connected consumer product" to a product's advertised functionality, and make various technical and clarifying changes.

This bill is supported by a variety of consumer advocacy groups, including Consumer Reports. Consumer Technology Association opposes the bill. Center for Democracy and Technology adopts a "support if amended" position, and a coalition of business associations led by the California Chamber of Commerce adopt an "oppose unless amended" position.

If passed by this committee, the bill will next be referred to the Judiciary Committee.

EXISTING LAW:

1) Provides that it is unlawful for any person doing business and advertising in this state to make any false or misleading advertising claim. (Bus. & Prof. Code § 17508.)

2) 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. (Civ. Code § 1792.)

3) Defines "connected device" to mean 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.)

4) Requires a manufacturer of a connected device to equip the device with a reasonable security feature or features meeting specified criteria. (Civ. Code § 1798.91.04.)

5) 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*.)

THIS BILL:

1) Defines the following terms:

   a) "Connected consumer product" to mean 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 for its functioning, in whole or in part, on a connection to the internet.

   b) "End of life" to mean the point after which the manufacturer no longer provides necessary support or security patches for a connected consumer product.

   c) "Manufacturer" to mean the manufacturer of a connected consumer product sold at retail in the state.

   d) "Minimum guaranteed support timeframe" to mean the minimum amount of time for which a company commits to providing all necessary support, security patches, or updates to a connected consumer product that includes a specific date at the end of the timeframe.

   e) "Necessary support" to mean all necessary support to enable product functionality.

2) Requires a manufacturer to clearly and prominently establish and disclose a minimum guaranteed support timeframe of a connected consumer product to any prospective buyer of the product, as provided.

3) Prohibits a manufacturer from reducing a minimum guaranteed support timeframe that has been disclosed to a prospective buyer.

4) Requires that a minimum guaranteed support timeframe established by a manufacturer be no less than 5 years.

5) Requires a manufacturer to provide notice to an owner of a connected consumer product both six months before and upon the 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.

6) Prohibits a manufacturer from requesting a product owner's contact information for any reason other than to provide a required notice.

7) 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 ensure that security patches provided by the manufacturer are promptly received and applied, and when the connected consumer product reaches its end of life, to notify the customer and replace the product with a comparable product that has not reached end of life.

8) Provides that a violation of the chapter constitutes a deceptive act or practice under UCL.

COMMENTS:

1) **Author's statement.** 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.

2) **Background.** *The internet of things.* The "internet of things" (IoT) refers to a network of devices, vehicles, appliances, and other physical objects that are embedded with sensors, software, and network connectivity, allowing them to collect and share data. Some examples are kitchen appliances, thermostats, door locks, home surveillance systems, or automated sprinklers.

According to IBM's website:

> IoT enables these smart devices to communicate with each other and with other internet-enabled devices. Like smartphones and gateways, creating a vast network of interconnected devices that can exchange data and perform various tasks autonomously. This can include:

- monitoring environmental conditions in farms
- managing traffic patterns with smart cars and other smart automotive devices
- controlling machines and processes in factories
- tracking inventory and shipments in warehouses

> The potential applications of IoT are vast and varied, and its impact is already being felt across a wide range of industries, including manufacturing, transportation, healthcare, and agriculture. As the number of internet-connected devices continues to grow, IoT is likely to play an increasingly important role in shaping our world. Transforming the way that we live, work, and interact with each other.[1]

Consumer products belonging to the IoT increasingly depend on software, cloud infrastructure, and remote services to function as advertised. Unlike traditional consumer goods, when a connected consumer product is no longer supported by its manufacturer, the product may become less secure, less functional, or entirely unusable despite the device itself remaining physically intact. As a result, the safety and useability of smart locks, security cameras, baby monitors, wireless speakers, household appliances, smart thermostats, and wearables are intrinsically tied to whether their manufacturers continue to provide security patches, software updates, and related support.

Ongoing support is especially important for cybersecurity. Connected products can collect sensitive information, control access to homes and networks, and communicate with other devices and cloud services. When manufacturers stop addressing known vulnerabilities, unsupported devices can become entry points into home networks, expose personal information, or be recruited into botnets and other attacks. A recent publication from the National Institute of Standards and Technology (NIST) describes cybersecurity issues associated with IoT and connected devices:

> As IoT adoption has increased over the last two decades, threats and vulnerabilities have also grown. For example, large, resilient botnets made up of compromised IoT devices (e.g., the Mirai botnet) resulted in a response from the United States Government in the form of Executive Order (EO) 13800. Since that time, there's been increasing acknowledgement of the importance of cybersecurity of IoT products and efforts to support and promote it. Even today, trust in IoT, which is supported by cybersecurity, is seen as a key factor to sustaining and amplifying the adoption and innovation of IoT products. Manufacturers should consider the cybersecurity of their IoT products to ensure customers can trust the products and their operation. Doing so can not only protect customers as they deploy and use IoT products, but manufacturers themselves by increasing trust in their products, supporting their reputation among customers, and reducing the likelihood of attacks on manufacturers' internal systems. Finally, considering cybersecurity in the development and support of IoT products protects

---

[1] IBM, *What is the IoT?* https://www.ibm.com/topics/internet-of-things.

the Nation, Internet, and public at large by reducing the likelihood of attacks utilizing IoT products (e.g., botnets).[2]

For purchasers of connected products, ongoing support is also central to whether the consumer receives the product they believed they were purchasing. Consumers cannot meaningfully compare products if they do not know for how long a connected device will remain safe and useable. According to the Federal Trade Commission many smart-product manufacturers fail to clearly disclose how long products will receive software updates, even though those updates help keep products secure and operating properly:

> You just bought a new "smart" lighting system that allows you to adjust the lighting of your home using your voice or remotely using an app. How long will the system last? Or you just paid for a "smart" blood glucose monitoring system that uses an app to keep track of your readings and to share them with your healthcare provider. How long will you or your doctor have access to your readings?
>
> The answer, according to a new study conducted by FTC staff is, "who knows?" FTC staff looked for information about the duration of software support commitments for 184 connected products, including smart phones, home appliances, health monitors, and fitness devices. The big takeaway from this study: **Nearly 89 percent of the manufacturers' web pages for these products failed to disclose how long the products would receive software updates.**[3]

Without clear disclosure, consumers may unknowingly purchase products that are nearing the end of support or that carry no meaningful support commitment. Other jurisdictions recognize the importance of this information; the United Kingdom's Product Security and Telecommunications Infrastructure Act 2022, for example, requires manufacturers to publish minimum security update periods:

> The three security requirements mandate that . . . a manufacturer must publicise the minimum period for which security updates will be provided for the product. This must be provided pro-actively in a clear, transparent, and understandable way to someone without prior technical knowledge. If the manufacturer's website or a website it controls contains an invitation to purchase a connectable product, the minimum security update period information must be published on that website.[4]

3) **What this bill would do.** This bill would require manufacturers of connected consumer products – products that rely on internet connectivity for their functionality – to support those products for a minimum of 5 years, and to disclose a product's support timeline to owners and

---

[2] NIST, "Foundational Cybersecurity Activities for IoT Product Manufacturers," (Apr. 2026), https://nvlpubs.nist.gov/nistpubs/ir/2026/NIST.IR.8259r1.pdf.
[3] FTC, "Smart Device Makers' Failure to Provide Updates May Leave You Smarting," *Staff Perspective,* (Nov. 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/smart-device-makers-failure-to-provide-software-updates-may-leave-you-smarting.pdf.
[4] Ashley Borthwick, Katie Simmonds, and Jenny Gibbs, "Cyber security for Internet of Things devices: a quick guide to the Product Security and Telecommunications Infrastructure Act," *Womble Bond Dickinson,* (Feb. 26, 2025), https://www.womblebonddickinson.com/uk/insights/articles-and-briefings/cyber-security-internet-things-devices-quick-guide-product-security/.

prospective purchasers of the product prior to sale, six months prior to support ending, and upon ending support for the product. The bill would additionally require businesses that lease out connected consumer products to ensure security patches are promptly applied, and to replace a connected consumer product that reaches its end of life during the lease with a comparable product capable of receiving necessary security patches, updates, and support, provided a comparable product is reasonably available.

Writing in support of SB 898, Consumer Reports describes the need for this measure:

> 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.

4) **Committee amendments.** Taking an "oppose unless amended" position, Civil Justice Association of California (CJAC) describes an issue arising from the bill's prohibition on reducing a minimum guaranteed support timeframe:

> …as currently drafted, [SB 898 creates] compliance obligations that manufacturers may be unable to meet through no fault of their own. We would support language to accommodate situations where reduction of a minimum support timeframe is not technically feasible or would interfere with efforts to prevent abuse, respond to legal requirements, or address security and operability issues . . . Legitimate circumstances that may require adjustment include unanticipated component end-of-life, supply chain failures, or technical constraints that only become apparent years after a product's initial release.

To address this concern, the author has agreed to an amendment allowing a manufacturer to reduce a minimum guaranteed support timeframe if the manufacturer "demonstrates that providing support for the product is not feasible due to unforeseeable circumstances beyond the manufacturer's reasonable control," including any of the following circumstances:

- The manufacturer files for bankruptcy.
- A third-party dependency is no longer available on commercially reasonable terms, and the manufacturer cannot reasonably replace it.
- Providing support is unlawful.

- The product is fundamentally unsafe or unsecure, and the issue cannot reasonably be remedied.

CJAC continues, describing an issue with the bill's inflexible 5-year guaranteed minimum support timeframe:

> Additionally, flexibility allowing manufacturers to establish different minimum guaranteed support timeframes for different models, versions, or product categories, provided such timeframes are clearly disclosed would also be helpful to ensure feasibility without disrupting the intent of the bill.

To address this concern, the author has agreed to an amendment removing the strict 5-year minimum requirement, and instead allowing a manufacturer to establish a timeframe that is "consistent with the reasonable expectations of a consumer" based on all of the following:

- The nature of the product.
- The price of the product.
- How the product is advertised.
- The minimum guaranteed support timeframes of comparable products.

Taking an "oppose unless amended" position, a coalition of industry associations led by the California Chamber Commerce describes an issue related to the scope of products covered under the bill:

> First and foremost, the term "connected consumer product" is overly broad, as a result of which the bill applies identical disclosure and replacement obligations to internet connective products with fundamentally different lifecycles, business models and pricing structures, and consumer relationships. Stated another way, the bill still applies to an extraordinarily diverse set of internet-dependent physical products. Realistically, obligations and remedies designed for one product can produce unworkable, disproportionate, if not absurd results when applied to another. To help address these concerns, we would suggest, at minimum, an amendment to limit the definition to products whose primary purpose depends on internet connectivity.

To address this concern, the author has agreed to an amendment limiting the scope of the bill to products that require internet connectivity for their "ordinary use," defined as "use 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."

Taking a "support if amended" position, Center for Democracy & Technology (CDT) requests that minimum guaranteed support timeframes under the bill be tied to a specific end date:

> For the minimum guaranteed product support time frame, we recommend a specified end date, as set forth in the Model Act. That way, the period will be clear and will not vary with

the purchase date of each product, which would create unnecessary burdens on both the manufacturer and the consumer to keep track of.

To address this concern, the author has agreed to an amendment clarifying in the definition of "minimum guaranteed support timeframe" that the timeframe begins "when a manufacturer first makes a connected consumer product available for purchase in this state" and ends "on a specific date."

Various groups raise technical feasibility concerns in response to the bill's notification and leasing requirements – to address these concerns, the author has agreed to make certain provisions of the bill apply only "to the extent technically feasible."

Paragraph (6) of subdivision (a) in Section 22928.11 prohibits manufacturers from requesting a connected consumer product owner's contact information for any purpose other than "providing a notification pursuant to this subdivision." In practice, this would prevent manufacturers from collecting shipping information, payment processing information, and information that is required to be collected pursuant to other laws – for example, information required to conduct a background check. To address this concern, the author has agreed to instead specify that nothing in the bill requires "a manufacturer to collect or retain contact information from the owner of a connected consumer product."

Finally, the author has agreed to various non-substantive cleanup amendments throughout. The full text of the bill as proposed to be amended follows:

SECTION 1. Chapter 28.6 (commencing with Section 22928.10) is added to Division 8 of the Business and Professions Code, to read:

CHAPTER 28.6. Connected Consumer Products

22928.10. As used in this chapter:

(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 **~~for its functioning, in whole or in part,~~** on a connection to the internet ***for a consumer to make ordinary use of the product***.

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

manufacturer commits to providing all ~~necessary~~ support, security patches, or updates ~~to~~ ***that are necessary for a consumer to make ordinary use of the product*** ~~**a connected consumer product that includes a specific date at the end of the timeframe**~~**.**

~~**(c) "Necessary support" means all necessary support to enable product functionality.**~~ ***(e) "Ordinary use" means use of a connected consumer product that is consistent with a consumer's reasonable expectations based on how the product was advertised, marketed, or otherwise described by the manufacturer at the time of purchase.***

22928.11. (a) A manufacturer shall clearly and ~~**prominently establish and**~~ ***conspicuously*** disclose ***a connected consumer product's minimum guaranteed support timeframe*** to any prospective buyer of ~~**a**~~ ***the*** ~~**connected consumer**~~ product ~~**a minimum guaranteed support timeframe**~~ **in** ~~**both**~~ ***all*** of the following ways***, to the extent each is technically feasible***:

(1) At the point of internet sale~~, if practicable~~.

(2) ~~**In a clear and conspicuous manner o**~~***O*****n** the product packaging**.**

(3) ~~**and o**~~***O*****n** the manufacturer's internet website or product-specific webpage.

(b) ***(1) Except as provided in paragraph (2),*** ~~**A**~~ ***a*** manufacturer shall not reduce a minimum guaranteed support timeframe disclosed under this section.

(2) (A) A manufacturer may reduce a minimum guaranteed support timeframe disclosed under this section only if the manufacturer demonstrates that providing support for the product is not feasible due to unforeseeable circumstances beyond the manufacturer's reasonable control, including any of the following:

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

(ii) 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.

(iii) Providing support is unlawful.

(iv) 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.

(B) A manufacturer that reduces a minimum guaranteed support timeframe pursuant to this paragraph shall, as soon as is practicable, provide clear and conspicuous notice to any affected consumers pursuant to subdivision (d).

(c) ~~**(1)**~~ A manufacturer shall ~~provide~~ ***ensure that the*** ~~**a**~~ minimum guaranteed support timeframe ***of a connected consumer product that it manufactured is consistent with the reasonable expectations of a consumer based on all of the following:***

(A) The nature of the product, including the product's expected use, durability, and reliance on remote services.

(B) The price paid for the product by consumers.

(C) How the product is advertised, marketed, or otherwise described by the manufacturer at the time of purchase.

(D) The minimum guaranteed support timeframes of comparable products ~~**of no less than five years**~~**.**

~~**(2) The starting point for the minimum guaranteed support timeframe shall be calculated from the first month in which the manufacturer offers the product for sale to consumers.**~~

(d) (1) A manufacturer shall provide a ***clear and conspicuous*** notice of a connected consumer product~~'s~~ ***reaching its*** end of life to the public and to any owner of the product on both of the following dates:

(A) Six months before the product reaches ***its*** end of life.

(B) The date on which the product reaches ***its*** end of life.

(2) A notification provided pursuant to this subdivision shall include both of the following:

(A) 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.

(B) A list of features lost, security risks, reduced interoperability, or any other changes ~~**that are**~~ likely to result from the connected consumer product~~'s~~ ***reaching its*** end of life.

(3) A notification provided pursuant to this subdivision shall be delivered in each of the following ways:

(A) Through an interface on the connected consumer product or associated application, if practicable.

(B) Through an email to the owner of a connected consumer product, if the manufacturer ~~possesses~~ ***knows*** the owner's email address.

(C) On the ***manufacturer's internet website or product-specific*** ~~connected consumer product's internet~~ webpage.

(4) A manufacturer shall ~~provide~~ ***allow*** a consumer ~~the means~~ to opt in to receive a notification pursuant to this subdivision through the connected consumer product's internet webpage.

(5) A notification ***provided*** pursuant to this subdivision shall be provided clearly and conspicuously as a standalone communication that ~~contains no~~***does not contain*** information unrelated to the notification.

(6*e*) ~~A manufacturer may request a connected consumer product owner's contact information solely for the purpose of providing a notification pursuant to this subdivision.~~*Nothing in this section shall be construed to require a manufacturer to collect or retain contact information from the owner of a connected consumer product.*

(~~e~~***f***) A business that owns or controls a connected consumer product that it leases or otherwise provides to ~~its~~ ***a*** customer~~s~~ as part of a service shall do ~~all~~ ***both*** of the following:

(1) ***To the extent technically feasible,*** ~~Ensure~~ ***ensure*** that security patches ~~provided~~ ***made available*** by the manufacturer for the connected consumer product are promptly ~~received and~~ applied ***to the product***.

(2) ~~When~~ ***If*** the connected consumer product ~~has reached~~***reaches*** its end of life, ***notify the customer and*** replace the connected consumer product, at no additional cost to the customer, with a comparable product ~~capable of receiving necessary security patches, updates, and support~~***that has not reached its end of life,*** if ***such*** a comparable product is reasonably available to the business.

~~**(3) Notify a consumer when the leased connected consumer product has reached its end of life.**~~

22928.12. A violation of this chapter constitutes a deceptive act or practice under the Unfair Competition Law (Chapter 5 (commencing with Section 17200) of Part 2 of Division 7).

5) **Further suggestions.** To ensure SB 898 remains both protective of consumers and technically feasible, the author may wish to consider the following additional amendments:

   a) Remove the explicit reference to California's UCL from Section 22928.12, as UCL applies to businesses regardless of whether a particular law specifically references it. The author may wish to strike this language from the bill to avoid the possibility of conflicting with UCL's default enforcement mechanisms.

   b) Clarify that "connected consumer product" refers to the physical product itself, rather than a mobile application or cloud infrastructure related to the functioning of the product. A manufacturer ceasing to support a mobile application or cloud infrastructure necessary for the ordinary use of a connected consumer product during the product's minimum guaranteed support timeframe would constitute a violation of this bill. The author may wish to strike "including a mobile application or cloud infrastructure related to the functioning of the physical product" from the definition of "connected consumer product" to clarify this point.

   c) Recast subdivision (c) of Section 22928.11 in terms of a requirement for a manufacturer to "***establish a minimum guaranteed support timeframe for any connected consumer product that it manufactures, and ensure that each minimum guaranteed support timeframe established pursuant to this section is consistent with the reasonable expectations of a consumer…"***

ARGUMENTS IN SUPPORT: California Public Interest Research Group writes in support:

At the moment, manufacturers design products that are totally reliant on internet connectivity and software support, but offer no information on how long consumers can expect that support to continue. Here are some reasons why passing SB898 is so critical for consumers:

1. **It would prevent electronic waste.** Last fall, Microsoft made the decision to end support for their Windows 10 operating system, despite previously describing it a "forever" version of Windows. This resulted in 400 million computers becoming electronic waste.

2. **It would prevent future cyberattacks.** When internet-connected devices stop receiving software support, they also stop receiving critical security updates that are needed to prevent malicious actors from compromising the device in the future. With millions of now "insecure" items now connected to the internet, these same malicious actors can use those devices to launch cyberattacks on other internet connected entities. Unsupported devices are a major security risk.

3. **It provides transparency for consumers.** Consumers currently have no way of knowing how long they can expect something they bought to be functional - they should.

Manufacturers should be clear about their plans for software support so everyday people aren't left in the lurch with a useless, insecure device.

ARGUMENTS IN OPPOSITION: Consumer Technology Association writes in opposition:

CTA supports initiatives that empower consumers with greater transparency, including meaningful information about the technology they purchase. However, CTA respectfully opposes SB 898 because, in its current form, the bill imposes disclosures that will create confusion for consumers, inconsistent compliance burdens for companies, and unintended market distortions. CTA supports consumer transparency regarding product lifecycle, security updates, and support commitments. When consumers understand how long products will receive updates and how vulnerabilities are managed, they can make better purchasing and security decisions. However, CTA believes that the mandatory disclosure regime in SB 898:

1. **Fails to align with federal and international frameworks** that provide standardized, actionable information to consumers across different products and markets.

2. **Mandates a blanket five-year minimum guaranteed support timeframe as a one-size fits all approach** for the broad scope of connected consumer products. The expected and appropriate support timeframe will vary product to product, and a specific minimum period of time cannot be mandated.

3. **May mislead consumers** by focusing narrowly on a "minimum guaranteed support time frame" without considering the complexity of modern connected products (e.g., cloud-based services, varying update mechanisms, and security patch schedules). Further, requiring that retailers, particularly small brick-and-mortar businesses, provide a comprehensive catalog of websites at the point-of-sale will no doubt result in consumers receiving outdated information even despite diligent compliance efforts.

4. **Covers too many products with unclear language.** Phrases like "in part" could unintentionally include devices that only indirectly connect to the internet. It also includes cloud infrastructure, which manufacturers typically don't control or update, so it should be excluded.

5. **Imposes compliance burdens on small and medium manufacturers,** particularly those selling across multiple jurisdictions with differing disclosure regimes, without clear evidence that these disclosures improve consumer outcomes.

6. **Requires manufacturers to notify device owners in ways that aren't practical.** Consumer electronics are often reused, resold, or donated, making it difficult to identify and contact current owners—especially beyond the original purchaser, and only if the product was registered. Requiring six months' advance notice is also unrealistic, as manufacturers may not know that far ahead when support or updates will end.

7. **Uses unclear standards for what counts as "notice."** Without clear guidance, it's uncertain what communication methods are acceptable. Requiring support timelines on packaging isn't practical because timelines can change after products are shipped.

Written notices years after purchase are also impractical, and adding separate printed materials creates unnecessary waste.

8. **Duplicates and potentially conflicts with emerging voluntary labeling systems** designed by federal policymakers and industry working together to present security and support information in a consumer-friendly way.

REGISTERED SUPPORT / OPPOSITION:

Support

CALPIRG, California Public Interest Research Group
Consumer Reports Advocacy
Fulu Foundation
Secure Resilient Future Foundation INC.
Software Freedom Conservancy

Opposition

Association of Home Appliance Manufacturers
Consumer Technology Association

Oppose Unless Amended
Advanced Medical Technology Association (ADVAMED)
California Chamber of Commerce
Civil Justice Association of California (CJAC)
Computer & Communications Industry Association
Entertainment Software Association
General Motors
Technet

Analysis Prepared by: Slater Sharp / P. & C.P. / (916) 319-2200