SENATE JUDICIARY COMMITTEE
Senator Thomas Umberg, Chair
2025-2026 Regular Session

SB 898 (Weber Pierson)
Version: March 24, 2026
Hearing Date: April 21, 2026
Fiscal: Yes
Urgency: No
AWM

SUBJECT

Connected consumer products

DIGEST

This bill, as the author agreed to amend it, requires manufacturers of connected consumer products to establish minimum guaranteed support timeframes for their products, which must be a minimum of five years, and to disclose support timeframes before purchase and as the product reaches its end of life.

EXECUTIVE SUMMARY

Consumer devices are increasingly connected to the internet. These connected consumer devices, sometimes referred to as "the Internet of Things," or IoT, encompasses a wide range of products, such as wearable health devices that report on the wearer's activity or sleep; refrigerators that can send a message to their owners when the milk is running low; e-readers; and a wide range of children's toys. Estimates suggest that there are tens of billions of IoT devices in use.[1]

The proliferation of connected devices raise two consumer concerns. First, unlike a traditional device, which lasts until its physical parts break, an IoT product can be "broken" when the manufacturer stops updating it or supporting its connected functionality. Consumers who pay for a connected device currently have no way of knowing how long it will be before their product turns into costly e-waste. Second, IoT devices have various levels of security. Existing law requires connected devices to be equipped with reasonable security features that are appropriate for the device, as provided. When manufacturers stop providing security updates and full functionality for these devices, however, security risks skyrocket, and there are concerns that

[1] Security Guide, *Internet of Things (IoT)*, NIST, https://www.nccoe.nist.gov/iot. All links in this analysis are current as of April 17, 2026.

consumers are not adequately informed when their beloved devices turn into security hazards.

This bill, as the author agreed to amend it in the Senate Privacy, Digital Technologies, and Consumer Protection Committee, requires manufacturers of connected consumer products to disclose to consumers a minimum guaranteed support timeframe, which must be at least five years, and to notify consumers as the product is reaching its end of life. The bill also requires businesses leasing or providing customers with such products to ensure the products are updated promptly and replaced when no longer supported. A violation of the bill's requirements constitutes a deceptive act or practice under the Unfair Competition Law (UCL), which allows an person injured by the proscribed practice to file a civil action for injunctive and equitable relief.

This bill is sponsored by the author and is supported by CALPIRG and iFixit. This bill is opposed by the Consumer Technology Association and the Civil Justice Association of California. The Senate Privacy, Digital Technologies, and Consumer Protection Committee passed this bill with a vote of 7-1.

PROPOSED CHANGES TO THE LAW

Existing law:

1) 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).)

2) Provides that, subject to the requirements in 1), 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).)

3) 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. (Civ. Code §§ 1798.91.05, 1798.06.)

4) 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).)

5) 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, div. 3, pt. 4, tit. 1.81.5, §§ 1798.100 et seq.)

6) 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. (Bus. & Prof. Code, div. 7, pt. 2, ch. 5, §§ 17200 et seq.)

7) 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.
    h) A person who has suffered injury in fact and has lost money or property as a result of the act of unfair competition. (Bus. & Prof. Code, § 17204.)

This bill, as the author agreed to amend it in the Senate Privacy, Digital Technologies, and Consumer Protection Committee:

1) Defines the following 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 used to support the functionality of a physical product.

   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 timeline.

2) Requires a manufacturer to clearly and prominently establish and disclose to any prospective buyer of a connected consumer product a minimum guaranteed support timeline 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 internet website or product-specific webpage.

3) Prohibits a manufacturer from reducing a minimum guaranteed support timeframe disclosed under 2).

4) Requires a manufacturer to provide a minimum guaranteed support timeframe of no less than five years.

5) 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 on both of the following dates:
   a) Six months before the product reaches end of life.
   b) The date on which the product reaches end of life.

6) Provides that a notification provided pursuant to 5) 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.

7) Requires the notice required under 5) to be provided in a separate document that contains no other information or notification.

8) Requires a business that owns or controls a connected consumer product that it leases or otherwise provides to consumers 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 consumer, with a comparable product capable of receiving necessary updates and support if a comparable product is reasonably available to the business.

9) Provides that a violation of 1)-8) constitutes a deceptive act or practice under the UCL.

COMMENTS

1. Author's comment

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 on the "Internet of Things"

The IoT broadly "encompasses everything connected to the internet, but is increasingly being used to define objects that 'talk' to each other."[2] IoT, or "smart," products, include products that can be managed and adjusted by the consumer via an app—such as an oven, blood glucose monitor, or even a hair dryer—as well as products that can be activated or adjusted without the consumer's involvement, such as Ring's "Search

[2] Burgess, *What is the Internet of Things? WIRED explains* (Feb. 16, 2018) WIRED, https://www.wired.com/story/internet-of-things-what-is-explained-iot/.

Party" function, an AI-powered surveillance tool which lets Ring activate a user's home surveillance camera and collect footage without the user's input.[3]

The upsides of IoT products are convenience and connectivity. For a consumer, the ability to start their dishwasher from their office, or to check on the baby monitor from a restaurant, can be a big selling point. Wearable technology, like smart watches, fitness trackers, sleep monitors, and other biometric trackers have exploded in popularity with people who want to track their own health metrics on a daily basis.[4]

IoT products also have their downsides, particularly privacy risks. An internet connection brings the risk of hacking. Internet-connected devices have several points of vulnerability, which can arise from the manufacturer's failure to implement adequate security measures or a user's own inattention to their security hygiene.[5] Because IoT products collect so much sensitive information, ranging from sensitive health information to video of the inside of a home, the cost of a data breach can be high, in terms of both financial losses (e.g., from stolen banking data) and the loss of feeling secure in your own home (e.g., from finding a video of yourself taken by your robot vacuum posted on the internet).[6]

Another downside of connected devices is the risk that the manufacturer will stop supporting the connected features of the device, degrading or ruining the product. As the Federal Trade Commission (FTC) explains:

> For non-connected devices, a product will last until it physically fails. Connected "smart" products, however, rely on software or an accompanying app, or both, to connect to the internet to operate. The software or app often needs to be updated to protect the device against security threats and to ensure continued connectivity. If the manufacturer stops providing these updates, the product may lose its "smart" functionality, become insecure, or completely cease to operate. Maybe the manufacturer will support the device forever, or maybe just for the same time period as the written warranty if one is offered. If a manufacturer fails to disclose how long it will support a product, consumers have no

---

[3] *E.g.*, Isaacs, *Ring's AI Pet Search Party Has The Internet Worries: Here's What To Know* (Feb. 11, 2026) Forbes, https://www.forbes.com/sites/forbes-personal-shopper/2026/02/11/ring-ai-search-party-privacy-concerns/.

[4] Wearable Technology Market Overview, Wearable Technology Market Size, Share, Growth, and Industry Analysis By Type (last updated Apr. 10, 2026) *available at* https://www.businessresearchinsights.com/market-reports/wearable-technology-market-119131.

[5] *E.g.*, Cohen, *Your Smart Home Is a Target for Hackers. Lock It Down With These Quick Tips* (Apr. 6, 2026) PCMag, https://www.pcmag.com/explainers/your-smart-home-is-a-target-for-hackers-lock-it-down-with-these-quick-tips.

[6] State of Surveillance, Your Robot Vacuum Is Mapping Your Home—And Sharing It (Dec. 12, 2025) *available at* https://stateofsurveillance.org/articles/surveillance/robot-vacuum-surveillance-mapping-your-home/.

> way of knowing how long the product will last—or how long it will work as intended or marketed.[7]

For example, in 2025, Google announced that it would stop supporting first- and second- generation Nest thermostats, thereby transforming homeowners' "smart" thermostats into dumb ones.[8] Google offered affected Nest users a "nearly 50% off" discount on a new Nest thermostat to affected consumers.[9] In terms of consumer expectations, the first- and second-generation models were released in 2011 and 2012, before Google bought Nest, so those homeowners did not get to choose whether they wanted to entrust Google with their thermostats.[10]

3. Understanding the risks of using IoT products after the manufacturer has ceased support

As explained by the Senate Privacy, Digital Technologies, and Consumer Protection Committee's analysis of this bill:

> 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

---

[7] FTC Bureau of Consumer Protection, Report: Smart Device Makers' Failure to Provide Updates May Leave You Smarting (Nov. 2024) *available at* https://www.ftc.gov/reports/smart-device-makers-failure-provide-updates-may-leave-you-smarting.
[8] *See* Google Nest Help, End of support for Nest Learning Thermostats (1st & Second gen), https://support.google.com/googlenest/answer/16233096?hl=en.
[9] *Ibid.*
[10] *See ibid.*; Oreskovic & Gupta, *Google gains entry to home and prized team with $3.2 billion deal* (Jan. 14, 2014) Reuters, https://www.reuters.com/article/technology/google-gains-entry-to-home-and-prized-team-with-32-billion-nest-deal-idUSBREA0C1HP/.

> 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.[11]

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.[]"[12]

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:

---

[11] 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.

[12] 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* (Mar. 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/.

> 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 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.[13]

4. <u>This bill, as the author agreed to amend it in the Senate Privacy, Digital Technologies, and Consumer Protection Committee, imposes specified disclosure and support requirements on the manufacturers of IoT products</u>

This bill is intended to provide consumers with information about how long a manufacturer will support an IoT product, or "connected consumer device." The bill requires manufacturers to provide consumer notice at three stages:

- Before purchase, when the manufacturer must clearly and prominently disclose their minimum support timeframe at the point of sale, if practicable, on the device packaging, and on their website.
- Six months before the product reaches the date when support will cease, also known as end of life, when notice must be given to the public and any owner of the product.
- The date on which the product reaches end of life; notice must again be given to the public and any owners of the product.

The bill specifies that a manufacturer's minimum support timeframe can be no less than five years. The author has agreed to amend the definition of "connected consumer device" and to clarify that the minimum support timeframe runs from the month and

[13] 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.

year that the manufacturer first offers the product for sale; these amendments are set forth in Comment 5, below.

The bill also 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.

The Senate Privacy, Digital Technologies, and Consumer Protection Committee considered this bill from an overall policy standpoint and passed it with a vote of 7-1. This Committee has jurisdiction over (1) the remedies created by the bill and (2) the First Amendment question that arises whenever the state compels commercial speech.

a. Remedies

Rather than creating a new enforcement mechanism, this bill provides that a violation of its requirements constitutes a deceptive act or practice under the UCL.

The UCL prohibits acts of unfair competition, which includes "any unlawful, unfair or fraudulent business act or practice and unfair, untrue or misleading advertising," and any act prohibited under the False Advertising Law.[14] The UCL does not establish an action for damages; instead, it establishes equitable remedies, plus the possibility of civil penalties in actions brought by specified public prosecutors.[15] Specifically, any person injured by an act of unfair competition may file a UCL action to obtain an injunction to stop the practice, and the court may also award restitution of any property obtained by means of the unfair competition.[16] The Attorney General, a district attorney, and specified city attorneys and county counsels from counties with a population in excess of 750,000 can also file UCL suit and obtain a civil penalty of up to $2,500 for each violation.[17] In assessing the amount of the civil penalty, the court shall consider the factors relevant to the case, including: "the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth."[18]

[14] Bus. & Prof. Code, § 17200.
[15] *Id.*, §§ 17203-17206.
[16] *Id.*, §§ 17203, 17204.
[17] *Id.*, § 17206(a).
[18] *Id.*, § 17206(b).

b. First Amendment analysis

"Commercial speech," including statements made in advertising, is protected by the First Amendment but enjoys a lesser degree of protection than other forms of constitutionally guaranteed expression.[19] "The First Amendment's concern for commercial speech is based on the informational function of advertising."[20] Advertising that is misleading or unlawful has no informational value and can be banned by the government.[21] But for an advertisement that "is neither misleading nor unrelated to unlawful activity, the government's power is more circumscribed."[22] To regulate accurate speech relating to legal activity, the government must assert a "substantial interest" to be achieved, and the limitation "must be designed carefully to achieve the State's goal."[23] When a state seeks to compel commercial speech, e.g., require an advertisement to disclose specific information, "a requirement that [an advertiser] include in [their] advertising purely factual and uncontroversial information" that will "dissipate the possibility of consumer confusion or deception" will generally pass First Amendment muster.[24]

The disclosures here appear reasonably tailored to achieve the important goals of (1) ensuring consumers are informed about the longevity of a product before they buy it, and (2) informing consumers when their products reach end of life. Given that an IoT product can become unsafe, or just plain useless, after the manufacturer stops supporting the product, the minimum guaranteed support timeframe is a crucial factor in determining whether the device is worth the price. And given that an unsupported connected device can put people's most intimate data at risk, warnings that a device is about to reach end of life and is, therefore, no longer safe will help consumers make informed choices about their devices.

5. Amendments

As noted above, the author has agreed to minor amendments to clarify the bill's scope. These amendments will be crossed along with the Senate Privacy, Digital Technologies, and Consumer Protection Committee's amendments. The amendments are set forth below, subject to any nonsubstantive changes the Office of Legislative Counsel may make.

---

[19] *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York* (1980) 447 U.S. 557, 562-563.
[20] *Id.* at p. 563.
[21] *Ibid.*
[22] *Ibid.*
[23] *Ibid.*
[24] *Zauderer v. Office of Disciplinary Counsel of Supreme Court of Ohio* (1985) 471 U.S. 626, 651.

Amendment 1

Amend the definition of "connected consumer product" to mean "any physical product, including any 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 connection to the Internet."

Amendment 2

In subdivision (c), add a new paragraph that reads "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."

6. Arguments in support

According to CALPIRG:

CALPIRG is an advocate for consumers, advancing solutions to problems that affect our health, our safety and our well-being, with thousands of members within the state of California. 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.

Passing SB898 would create more transparency around software support and would hold manufacturers accountable for prematurely ceasing needed software updates. We urge you to approve and pass SB898 this session.

7. Arguments in opposition

According to the Consumer Technology Association:

> 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. **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.
> 3. **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.
> 4. **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.

SUPPORT

CALPIRG
iFixit

OPPOSITION

Consumer Technology Association
Civil Justice Association of California

RELATED LEGISLATION

Pending legislation: AB 1921 (Ward, 2026) requires digital games available for purchase on or after January 1, 2027, to communicate specified information to users 60 days before the operator ceases to provide services necessary for the ordinary use of the game, and to require the operator to take specified steps upon the date it ceases to provide services necessary for ordinary use. AB 1921 is pending before the Assembly Judiciary Committee.

Prior legislation:

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

PRIOR VOTES

Senate Privacy, Digital Technologies, and Consumer Protection Committee (Ayes 7, Noes 1)

****