Date of Hearing: April 21, 2026
Fiscal: No

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
AB 2062 (Patterson) – As Amended March 19, 2026

PROPOSED AMENDMENTS

SUBJECT: Security cameras: access and use of content

SYNOPSIS

In what is potentially one of the most spectacular advertising failures in recent memory, during the recent 60th Super Bowl game, Ring released a 30-second ad about their new feature, entitled Search Party. In the ad, a young girl finds her missing dog, Milo, by connecting to other Ring doorbell cameras in an idyllic suburban neighborhood. Strolling along the street, Jamie Siminoff, Ring's founder, proclaims: "Be a hero in your neighborhood with Search Party".

This bill, while not the direct result of that ad, might be considered part of the fallout from it. The author notes:

> *The recent situation with Ring shows the need for this bill. Ring created an opt-out feature that would automatically take footage from customers, send it to the web, and use the footage, in conjunction with AI, to find pets. At the same time, Ring announced a partnership with Flock, a company that supplies police departments with license-plate readers and security cameras, to make it easier for Ring customers to send footage to law enforcement departments. This raised privacy concerns, as customers were worried that their data would be sent to Flock through this opt-out feature.*

This bill prohibits home security companies from distributing, selling, or providing access to the content from home security cameras without first obtaining the consent of the consumer. The bill is supported by Oakland Privacy.

Committee amendments, described in Comment #5, are largely clarifying in nature. They add definitions, update some of the terms used, and otherwise ensure that the intent of the bill is clear.

EXISTING LAW:

1) Provides, pursuant to the U.S. Constitution, that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized." (U.S. Const., Fourth Amend; *see also* Cal. Const. art. 1, § 13.)

2) Provides, pursuant to the California Constitution, that all people are free and independent by nature and have inalienable rights. Among these is the fundamental right to privacy. (Cal. Const. art. I, § 1.)

3) States that the "right to privacy is a personal and fundamental right protected by Section 1 of Article I of the Constitution of California and by the United States Constitution and that all individuals have a right of privacy in information pertaining to them." Further states these findings of the Legislature:

    a) The right to privacy is being threatened by the indiscriminate collection, maintenance, and dissemination of personal information and the lack of effective laws and legal remedies.

    b) The increasing use of computers and other sophisticated information technology has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information.

    c) To protect the privacy of individuals, it is necessary that the maintenance and dissemination of personal information be subject to strict limits. (Civ. Code § 1798.1.)

4) Establishes the California Invasion of Privacy Act. (Pen. Code, § 630 et. seq.)

5) Prohibits tapping into a telephonic communication system (wiretapping), as specified, without the consent of all parties. (Pen. Code, § 631, subd. (a).)

6) Enacts the California Electronic Communications Privacy Act (CalECPA), which generally prohibits a government entity from compelling the production of or access to electronic communication information from a service provider or to electronic device information from any person or entity other than the authorized possessor of the device, absent a search warrant, wiretap order, order for electronic reader records, or subpoena issued pursuant to specified conditions, or pursuant to an order for a pen register or trap and trace device, as specified. (Pen. Code § 1546 et seq.)

7) Establishes the California Consumer Privacy Act (CCPA). (Civ. Code §§ 1798.100-1798.199.100.)

8) Prohibits a business from selling or sharing the personal information of a child that is 16 years of age or younger, if the business has actual knowledge of the child's age, unless the child, or the child's parent or guardian in the case of children less than 13 years old has affirmatively authorized the sharing of selling of the personal information. (Civ. Code § 1798.120(c).)

9) Provides a consumer, subject to exemptions and qualifications, various rights, including the following:

    a) The right to know the business or commercial purpose for collecting, selling, or sharing personal information and the categories of persons to whom the business discloses personal information. (Civ. Code § 1798.110.)

    b) The right to request that a business disclose the specific pieces of information the business has collected about the consumer, and the categories of third parties to whom the personal information was disclosed. (Civ. Code § 1798.110.)

c) The right to request deletion of personal information that a business has collected from the consumer. (Civ. Code § 1798.105.)

d) The right to opt-out of the sale of the consumer's personal information if the consumer is over 16 years of age. (Sale of the personal information of a consumer below the age of 16 is barred unless the minor opts-in to its sale.) (Civ. Code § 1798.12.)

e) The right to direct a business that collects sensitive personal information about the consumer to limit its use of that information to specified necessary uses. (Civ. Code § 1798.121.)

f) The right to equal service and price, despite the consumer's exercise of any of these rights, unless the difference in price is reasonably related to the value of the customer's data. (Civ. Code § 1798.125.)

10) Requires a business to provide clear and conspicuous links on its homepage allowing consumers to opt-out of the sale or sharing of their personal information and use or disclosure of their sensitive personal information. (Civ. Code § 1798.135(a).)

11) Defines the following terms under the CCPA:

a) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes such information as:

i) Name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, or other identifier.

ii) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

iii) Biometric information.

iv) Internet activity information, including browsing history and search history.

v) Geolocation data.

vi) Audio, electronic, visual, thermal, olfactory, or similar information.

vii) Professional or employment-related information. (Civ. Code § 1798.140(v).)

b) "Sensitive personal information" means personal information that reveals a person's:

i) Social security, driver's license, state identification card, or passport number.

ii) Account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials.

iii) Precise geolocation.

iv) Racial or ethnic origin, citizenship or immigration status, religious or philosophical beliefs, or union membership.

v) Email, mail and text messages.

vi) Genetic data.

vii) Information collected and analyzed relating to health.

viii) Information concerning sex life or sexual orientation. (Civ. Code § 1798.140(ae).)

12) Establishes the Unfair Competition Law, 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) Prohibits security camera companies, as defined, from distributing, selling, or otherwise authorizing a third party to access, use, or distribute content obtained from a consumer's security camera without first obtaining the consumer's consent.

2) Prohibits a security camera company from, by default, opting a consumer in to any feature that would allow the distribution, sale, or otherwise authorizing a third party to access, use, or distribute content obtained from a consumer's security camera.

3) Defines the following terms:

   a. "Content" means video, images, or data obtained from a security camera.

   b. "Security camera" means a device that is sold to monitor property or a structure for security purposes that captures or records videos or images that can be viewed live or reviewed later.

   c. "Security camera company" means an entity that sells security cameras or monitors content obtained from a security camera.

COMMENTS:

1) **Author's statement**. According to the author:

> California has consistently taken steps to protect the privacy of its residents. One important area that needs further consideration is regulation for security camera systems. Security cameras, particularly in people's homes, document some of the most personal moments that people have. Unfortunately, the law allows this footage to be shared with third-parties unless customers opt-out. AB 2062 requires these companies to have customers opt-into the system instead, ensuring that permission is given before footage is shared.

2) **The commercial that alarmed the country.** During the recent 60th Super Bowl performance, Ring released a 30-second ad about their new feature, entitled Search Party, which allowed a

young girl to find her missing lab, Milo, by connecting to other Ring doorbell cameras in the neighborhood. Jamie Siminoff, Ring's founder, proclaimed in the ad: "[b]e a hero in your neighborhood with Search Party" as he strolled through an idyllic suburban neighborhood. The backlash was swift.[1] The jump from surveilling the neighborhood for a missing dog to surveilling for petty criminals or even undocumented persons was obvious for some, who flooded YouTube comments for the ad with statements about "dystopian" futures and doubting whether the intent of Search Party extended only to finding lost dogs.[2] YouTube commentors were right to question the goal of Search Party. Although advertised as a helpful tool for uniting owners with their lost pets, internal emails from the company reveal that Siminoff's plans for Search Party go beyond finding missing dogs. In October, Siminoff emailed all Ring employees that the new feature would soon be able to "zero out crime in neighborhoods."[3]

3) **Impact of the growing use of personal surveillance cameras on Californians' privacy.** According to a 2026 home security survey, 61% of U.S. households now have at least one security camera — up from 52% in 2024. That equates to approximately 74.9 million homes having indoor or outdoor security cameras. Home security camera adoption has climbed 19 percentage points over two years, crossing the threshold from a minority to a majority. Video doorbell cameras have followed a similar arc, approaching half of all U.S. households at 48 percent, which equates to 58.9 million homes.[4]

Home surveillance cameras can be helpful security tools that protect families. However, when they are used for other purposes or as part of a broader surveillance network, there can be significant tradeoffs in terms of Californians' privacy. The technology captures the movements of people both in public and in their homes on recorded and live video feeds that can be accessed by hackers, the companies making the technology, and can be shared broadly. As an example of their risk to people's expectation of privacy, in 2022, the city of San Francisco embarked on a citywide surveillance experiment that explicitly allows law enforcement to access the live footage of privately owned internet cameras without first obtaining a court order or warrant.[5] Prior to the passage of the local ordinance, law enforcement could request previously recorded footage from the owners of internet cameras or ask the surveillance technology companies for data, but they could not tap into the live feeds of privately owned cameras.

Not only does the proliferation of these devices increase government surveillance, it also greatly increases the ability for individuals to hack into the cameras to gain access to private videos. In May 2023, the Federal Trade Commission (FTC) issued a consumer alert warning to people that these systems presented a privacy risk. According to the alert:

---

[1] Jordyn Holman, "Ring's Founder Knows You Hated That Super Bowl Ad," *The New York Times,* (Feb 19, 2026), https://www.nytimes.com/2026/02/19/business/ring-super-bowl-ad-privacy.html.
[2] Jason Koebler, "With Ring, American Consumers Built a Surveillance Dragnet," *404 Media,* (Feb 10, 2026), https://www.404media.co/with-ring-american-consumers-built-a-surveillance-dragnet/?ref=daily-stories-newsletter
[3] Jason Koebler, "Leaked Email Suggests Ring Plans to Expand 'Search Party' Surveillance Beyond Dogs," (Feb 18, 2026), https://www.404media.co/leaked-email-suggests-ring-plans-to-expand-search-party-surveillance-beyond-dogs/?ref=daily-stories-newsletter.
[4] Rob Gabriele, *2026 Home Security Market Report*, SafeHome.org (Apr. 1, 2026) https://www.safehome.org/resources/home-security-industry-annual/.
[5] *News Release - Board of Supervisors Approves Camera Access Legislation to better Protect Residents, Businesses, and Neighborhoods*. Office of the Mayor (Sep 21, 2022) *available at* https://sfmayor.org/article/board-supervisors-approves-camera-access-legislation-better-protect-residents-businesses-and.

> The FTC says Ring's poor privacy and lax security let employees spy on customers through their cameras, including those in their bedrooms or bathrooms, and made customers' videos, including videos of kids, vulnerable to online attackers. Hackers exploited those vulnerabilities and harassed, insulted, and propositioned children and teens through their Ring cameras. Some hackers even live streamed customers' videos.

Ultimately, Ring settled the case by agreeing to delete the misappropriated videos, establish a privacy and security program, and pay $5.8 million to affected customers. [6]

Supporting the bill, Oakland Privacy, raises the following concerns related to the proliferation of security cameras:

> Consumers install home security cameras in order to protect their property and feel insulated against threats like home invasion, burglary and package theft. The cameras are popular and it is estimated that 61% of American homes now have some kind of security camera system installed. But these cameras are not without privacy risks as demonstrated by the recent South Korean case where a gang of four hackers infiltrated 120,000 cameras in search of sexual content to sell to porn sites.
>
> [. . .]
>
> There are a large amount of home security devices for sale in California and they have varying degrees of technical proficiency. As the South Korea case demonstrates, some brands sold to consumers are not necessarily secure against external invasion. Similarly, the data collected by such cameras which is often far more extensive than simply the audio and video footage the device collects is usually conveyed back to the manufacturer in some form.
>
> Among the apps that collect the most data, Deep Sentinel and Lorex stand out for outdoor security cameras, each collecting 18 out of a possible 32 data points. Nest Labs, which leads the pack for indoor cameras, collects 17 data points, with Ring and Arlo each gathering 15. 3
>
> All of these companies have fairly permissive privacy policies which allow the provision of personal information to third party service providers, and to the companies themselves for some direct marketing services. For example, Nooie, a Milpitas company that manufactures indoor security cameras with motion tracking and smart home functions offers users a "right" to opt out of direct marketing on their rather hard to find privacy policy on their website.

In 2024, *Consumer Reports* released a report warning that video doorbells can be easily hacked. According to the findings, video doorbells sold on websites for Walmart, Amazon, Temu, Sears, and Shein could be easily taken over by someone who has physical access to the doorbells, create an account on a smartphone app and pairs the doorbell with their phone. The individual can then become the "owner" of the doorbell and have the ability to see those who arrive and those who leave.[7] This presents a serious risk to the privacy of anyone coming and going from

---

[6] Puig, Alvaro. *Ring's privacy failures led to spying and harassment through home security cameras.* FTC Consumer Advice (May 31, 2023) *available at* https://consumer.ftc.gov/consumer-alerts/2023/05/rings-privacy-failures-led-spying-and-harassment-through-home-security-cameras.

[7] Higginbotham and Wroclawski. "These Video Doorbells Have Terrible Security. Amazon Sells Them Anyway." *Consumer Reports* (Feb 29, 2024) *available at* https://www.consumerreports.org/home-garden/home-security-cameras/video-doorbells-sold-by-major-retailers-have-security-flaws-a2579288796/

the home. Perhaps more importantly, these technological weaknesses could be dangerous for people who are victims of stalking or intimate partner violence who installed these cameras thinking that they add an additional layer of security.

4) **Committee priorities.** The use of global positioning system (GPS) technology on phones and in cars, combined with a growing network of public and private surveillance cameras, including home security cameras, means that it is increasingly unlikely that people can step outside their homes without having their every movement tracked by private companies, their neighbors, and their government. This complete erosion of any expectation that people can maintain some semblance of privacy while in public and semi-public spaces, is a significant policy question that deserves serious consideration.

As both private and government surveillance have increased in the last few years, sometimes with alarming consequences, the Committee has focused on the implications of this loss of privacy, both through an informational hearing on mass surveillance and bills carried by Committee members on protecting sensitive personal information, surveillance pricing, location tracking, and the surveillance of workers in their workplace, to name a few. This bill, by banning the dissemination of private security footage without first obtaining consent, is another important step in trying to help Californians regain some of their privacy.

5) **Amendments.** The author has agreed to the following amendments that do not change the intent of the bill, they are largely definitional and clarifying:

22949.100. (a) For purposes of this chapter:

(1) "Content" means video, images, ***audio*** or ***other*** data obtained from a security ***surveillance system*** ~~cameras~~.

~~(2) "Security camera" means a device that is sold to monitor property or a structure for security purposes that captures or records videos or images that can be viewed live or reviewed later.~~

(~~3~~***2***) ***(A) "Express consent" means an affirmative written authorization that is granted in response to a notice that is both of the following:***

(i) Clear, meaningful, and prominent.

(ii) Conveyed in a manner that a natural person would notice and understand it.

(B) "Express consent" does not include an authorization that is any of the following:

(i) Inferred from inaction.

(ii) Obtained through the use of a dark pattern, as defined in Section 56.18 of the Civil Code.

(iii) Contained within a more general notice, agreement, or set of terms and conditions.

(3) "Security ~~camera~~ ***surveillance*** company" means an entity that ***installs,*** sells ***or leases*** security ***surveillance systems for residential properties, including but not limited to self-installed security systems. A security surveillance company may also store data*** ~~cameras or~~

monitors content obtained from a security ***surveillance system or provide any other service associated with residential surveillance.*** ~~camera~~.

(4) "Security surveillance system" is any video, audio, or photographic recording devices installed for the purpose of surveilling or recording activity occurring at a residential property.

(5) "Third party" means a person who is not any of the following:

(A) The business with whom the consumer intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under this title.

(B) A service provider to the business.

(C) A contractor.

(b) A security ~~camera~~ ***surveillance*** company shall not distribute, sell, or otherwise authorize a third party to access, use, or distribute content obtained from a consumer's security ~~camera~~ ***surveillance system*** without first obtaining the ~~consumer's~~ ***express*** consent ***of the consumer and the adult residents of a residential rental property or upon receipt of an order of a Court, including a subpoena, or arbitrator.***

(c) A security ~~camera~~ ***surveillance*** company shall not, by default, opt a consumer in to any feature that would distribute, sell, or otherwise authorize a third party to access, use, or distribute content obtained from a consumer's security ~~camera~~ ***surveillance system***.

REGISTERED SUPPORT / OPPOSITION:

Support

Oakland Privacy

Opposition

None on file.

Analysis Prepared by: Julie Salley / P. & C.P. / (916) 319-2200