Date of Hearing: July 1, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 690 (Caballero) – As Amended May 29, 2025

PROPOSED AMENDMENTS

SENATE VOTE: 35-0

SUBJECT: Crimes: invasion of privacy

SYNOPSIS

The California Invasion of Privacy Act (CIPA) was adopted in 1967 to criminalize wiretapping, eavesdropping, interception, and recording of telephone communications without authorization from a court. CIPA also provides a private right of action for people injured by violations of its provisions. In adopting the statute, the Legislature recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . has created a serious threat to the free exercise of personal liberties." While CIPA expressly focuses on telephonic communications, it also uses broad, technology-neutral terms that courts have construed to apply to online communications.

CIPA has been a focal point in a recent surge of litigation related to third-party tracking of website user information. Three statutes in particular are implicated: Penal Code section 631, which applies to wiretapping; section 632, which applies to recordings of confidential communications; and section 638.51, which applies to pen registers and trap and trace devices. While the first two statutes date back to CIPA's inception and have long been understood to apply, albeit somewhat awkwardly, to online communications, the latter statute was added in 2015, with little, if any, thought given to its application to online activity and its interaction with CIPA's private right of action.

The pen register statute has become a poster child for abusive lawsuits. Enterprising plaintiffs' attorneys have exploited the statute at scale to go after businesses using third-party software to enable advertising on their websites. Because the potential liability can be staggering, businesses generally settle this litigation hastily, encouraging vexatious litigants to continue blasting out demand letters. Section 631, which is more difficult to assert, has also featured in this litigation, although to a lesser extent. And section 632 has not been used in these cases nearly as often. Whereas pen register violations typically involve seemingly innocuous technical violations arising from ordinary operation of websites, cases under the other two statutes often involve highly offensive intrusions on users' reasonable expectations of privacy, although they are not immune to abuse.

The bill in print seeks to provide relief to businesses, but does so with too blunt of a solution: it broadly exempts any "commercial business purpose" as defined by the California Consumer Protection Act (CCPA) from all civil and criminal liability under CIPA, potentially shielding genuine privacy violations in order to serve the laudable goal of enabling businesses to operate websites in a normal fashion. The Public Safety Committee previously heard the bill and passed it on a 9-0 vote.

The bill is sponsored by the Alliance for Legal Fairness and supported by businesses and trade associations from virtually every sector of the economy, who contend that it is necessary to staunch an inundation of litigation under outmoded statutes that were never intended to apply to website activity. They argue the CCPA, not CIPA, should govern online commercial activities.

The bill is opposed by a broad array of privacy, civil society, legal, and immigrant rights organizations, who contend that the bill undermines key protections against privacy violations – in particular, surreptitious interception of information by undisclosed third parties, which can lead to sensitive information of targeted individuals falling into the wrong hands – that the CCPA's opt-out regime is ill equipped to address.

Recognizing that the pen register statute is on a fundamentally different footing from the other two statutes, the author has agreed to amend the bill to address that statute only. As described in Comment #7, the amended bill, in its entirety, will simply eliminate the private right of action against private actors for violations arising from conduct occurring on websites. To provide relief to distressed businesses that are the subjects of currently pending pen register litigation, the bill applies these changes retroactively. In lieu of private standing, the Attorney General would be authorized to enforce these violations.

This does not mean there are no lingering problems with CIPA. Far from it; Section 631, in particular, continues to be challenging for courts to apply in this context. But it remains a key protection that warrants a more nuanced approach than a broad exemption. In the meantime, the solution the author has agreed to responds directly and surgically to the most pressing problem at hand. The elimination of the private right of action for pen register violations does not appear to have a substantial impact on individual recourse for surreptitious surveillance, which can still be pursued under other statutes. Going forward, however, the Legislature may wish to consider a more comprehensive set of solutions that provide courts, consumers, and businesses clearer guidance and strike the right balance between privacy interests and the realities of the modern internet.

EXISTING LAW:

1) 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.)

2) Establishes the CCPA. (Civ. Code §§ 1798.100-1798.199.100.)

3) 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.)

4) Defines "personal information" under the CCPA as 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:

a) 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.

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

c) Biometric information.

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

e) Geolocation data.

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

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

5) Defines "business purpose" as the use of personal information for the business' operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected. (Civ. Code § 1798.140(e).)

6) Specifies that "business purpose" includes:

a) Auditing related to counting ad impressions to unique visitors, verifying positioning and quality of ad impressions, and auditing compliance with this specification and other standards.

b) Helping to ensure security and integrity to the extent the use of the consumer's personal information is reasonably necessary and proportionate for these purposes.

c) Debugging to identify and repair errors that impair existing intended functionality.

d) Short-term, transient use, including, but not limited to, non-personalized advertising shown as part of a consumer's current interaction with the business, provided that the consumer's personal information is not disclosed to another third party and is not used to build a profile about the consumer or otherwise alter the consumer's experience outside the current interaction with the business.

e) Performing services on behalf of the business, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, providing storage, or providing similar services on behalf of the business.

f) Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.

g) Undertaking internal research for technological development and demonstration.

h) Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business. (Civ. Code § 1798.140(e)(1)-(8).)

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

8) Makes it a crime to intentionally and without the consent of all parties eavesdrop or record a confidential communication. (Pen. Code § 632(a).)

9) Defines "confidential communication" as "any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering or in any legislative, judicial, executive or administrative proceeding open to the public, or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded." (Pen. Code § 632 (c).)

10) Prohibits, without the consent of all parties, intercepting or receiving and intentionally recording a communication between two cellular phones. (Pen. Code § 632.7(a).)

11) Prohibits the interception of electronic communications and prohibits the installation or use of a pen register or a trap and trace device without first obtaining a court order, except as specified. (Pen. Code § 638.51(a) & (b).)

12) Defines a "trap and trace device" as a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication but not the contents of a communication. (Pen. Code § 638.50(c).)

13) Defines a "pen register" for these purposes to mean a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted but not the contents of a communication, with specified exceptions. (Pen. Code, § 638.50(b).)

14) Authorizes a person who has been injured by a violation of CIPA's prohibitions to bring an action against the person who committed the violation to enjoin and restrain the violation, as well as to bring an action for monetary damages, as specified. (Pen. Code, § 637.2.)

THIS BILL: Exempts any "commercial business purpose" as defined by the CCPA from civil and criminal liability pursuant to the provisions of CIPA that prohibit wiretapping, eavesdropping on, or recording confidential communications, intercepting and recording cellular communications, or using a pen register or trap and trace device.

COMMENTS:

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

> SB 690 will stop abusive shake down lawsuits for standard online business activities against California businesses and nonprofits filed under Section 638.51 of the California Invasion of Privacy Act (CIPA) enacted in 1967, long before the internet was even developed. In recent years, a small number of law firms have filed vexatious lawsuits inappropriately using CIPA's pen-register provision to prey on small business owners and non-profits who cannot afford the costs of litigation, but could afford to settle for a couple thousand dollars. SB 690 will clarify that private right of action within the pen-register provision of CIPA cannot be used against standard website operations.

2) **CIPA litigation surge.** Adopted in 1967, CIPA criminalizes wiretapping, eavesdropping, interception, or recording of telephone communications without authorization from a court.[1] CIPA's preamble states that "[t]he Legislature by this chapter intends to protect the right of privacy of the people of this state."[2] The Legislature recognized that "the development of new devices and techniques for the purpose of eavesdropping upon private communications . . . has created a serious threat to the free exercise of personal liberties."[3] The California Supreme Court,

---

[1] Pen. Code, § 630, *et seq*. All further statutory references are to the Penal Code unless otherwise indicated.
[2] *Ibid.*
[3] *Ibid.*

which "regularly reads statutes to apply to new technologies,"[4] has directed courts to "fulfill[] the legislative purpose of CIPA by giving greater protection to privacy interests."[5]

Section 637.2 confers a private right of action on "[a]ny person who has been injured by a violation of [CIPA]." Relief includes (1) statutory damages of $5,000 per violation; (2) three times the actual damages suffered by the plaintiff, if any; and (3) injunctive relief."[6] The statute specifically provides that a plaintiff need not have suffered, or been threatened with, actual damages[7] – that is, cognizable harms such as emotional distress, reputational damage, or identity theft beyond the mere violation of the statute.[8] Applied in the context of online tracking violations can stack up rapidly, causing defendants to face potentially devastating liability.

The Alliance for Legal Fairness, sponsors of the bill, describe a recent surge in litigation under CIPA:

> **Trial lawyers are targeting entities that are too small to fight back**
>
> When this effort began in early 2025, about 600 lawsuits had been filed against California businesses. Now, just 18 months later, that number has exploded to 4,000. Tens of thousands more have received demand letters telling businesses that the mere existence of a website has triggered criminal liability and thousands (if not millions) in damages owed to individuals who: a) have not suffered any injury or harm; b) are not existing customers; and c) do not have any connection to the business at all. These bad actors are actively creating legal chaos and a cottage industry of frivolous litigation.
>
> Defendants include businesses like Howdy Plumbing and Sweet E's Bakeshop, nonprofits like the Sacramento Food Bank, healthcare providers like Southern Mono Healthcare, and even public agencies like the Metropolitan Transit Authority of Los Angeles. Trial lawyers find clusters of companies in a geographic area and then paper all of them with demand letters. In the Sacramento area, one Los Angeles law firm targeted approximately 40 plumbing and HVAC companies. The law firm is a solo practice, the plaintiff in all 40 cases is another lawyer, and neither lawyers were customers of the Sacramento companies – they simply visited websites, sent demand letters accusing these businesses of criminal conduct, and expected the businesses to settle out of fear and confusion.
>
> **Litigation exposure adds up quickly**
>
> Importantly, these lawsuits do not require any proof of actual consumer harm to proceed and include $5,000 statutory damages per violation. There is no limit to the number of lawsuits a business or nonprofit can face. Under CIPA's private right of action, organizations can face

---

[4] *In re Google Inc*., (N.D. Cal. Sept. 26, 2013) No. 13-MD-02430, 2013 U.S. Dist. LEXIS 172784, 2013 WL 5423918, at *21.
[5] *Flanagan v. Flanagan* (Cal. 2002) 27 Cal. 4th 766, quoted in *Matera v. Google Inc*., (N.D. Cal. Aug. 12, 2016) No. 15-cv-04062, 2016 U.S. Dist. LEXIS 107918, 2016 WL 8200619, at *19.
[6] *See* § 637.2 (a)(1-2)-(c).
[7] §637.2(c).
[8] Importantly, the statute does not make actual harm a prerequisite for bringing suit. Such harms are often far downstream from the initial violation, meaning that a harm requirement significantly undermines any statutory remedies. However, it is important to ensure that violations involve circumstances that entail substantial privacy intrusions that fall outside of normal conduct. As described below, the pen register statute does not appear to meet this threshold.

> statutory damages of a minimum of $5,000 per website visit, with settlement demands ranging from $20,000 to as high as $5 billion. Accordingly, this has created massive financial exposure to nearly every California business from a legal trap.
>
> The combination of these factors has incentivized a small group of law firms to rely on a limited pool of repeat plaintiffs who file dozens of nearly identical cases – similar to ADA lawsuits – against the businesses and organizations that make up significant sectors of California's economy. One notable recent entrant into this feeding frenzy is a nonlawyer who has filed over 100 pro se claims in the past several months; he is a convicted felon who has served a federal sentence for extortion.

3) **Tracking for online advertising.** At the heart of the surge in litigation is the collection of information on websites in order to auction off ad space on websites and apps – a process known as "real-time bidding." According to an article from the International Association of Privacy Professionals:

> Real-time bidding is an advertising auction system that operates in the milliseconds it takes for a website or app to load. However, unlike a typical auction, where a winning bidder walks away with a product, real-time bidding leaves every participant holding something: your data.
>
> This includes IP addresses, device type, geolocation — down to a few meters — unique advertising ID, browsing behavior, and often inferred sensitive characteristics like political interests, health conditions or sexual orientation. These data points — known collectively as bidstream data — are shared with dozens, sometimes hundreds, of companies in a single transaction. Each time an ad loads, this entire process repeats. It happens billions of times per day.[9]

Ad tech companies, which include smaller companies as well as giants like Google, Meta, and Oracle, facilitate this process by serving as intermediaries between advertisers and the owners of websites (or apps). When a user visits the website, information about the users and the content they are viewing is sent to the ad tech company. The ad tech company packages information about the user into a "bid request," which is then sent to potential advertisers. Advertisers use the bid request and cradle-to-grave profiles they have compiled about the user to decide whether to bid on the ad space. The highest bidder gets to display an ad, but all of the advertisers collect the information from the request. Anyone can pose as an ad buyer. Data brokers often use this as a means of harvesting information at scale.[10]

In order to facilitate ad buying, website operators commonly embed an ad tech company's software on the operator's webpage. Once embedded, this software directly transmits information to the ad tech company. A recent legal guidebook describes common mechanisms for transmitting information:

---

[9] "Reassessing where real-time bidding fits into the risk landscape" (April 8, 2025), https://iapp.org/news/a/reassessing-where-real-time-bidding-fits-into-the-risk-landscape.
[10] Len Coehn, "Google Settlement May Bring New Privacy Controls for Real-Time Bidding," (Jan. 29, 2026), https://www.eff.org/deeplinks/2026/01/google-settlement-may-bring-new-privacy-controls-real-time-bidding.

> *Cookies* are text files placed on a user's browser to store information about user preferences, login credentials, and browsing activity. First party cookies are set by the website a user visits directly, whereas third-party cookies originate from external domains, often serving advertising and tracking purposes. [. . .]
>
> *Tracking pixels*, also known as web beacons or pixel tags, are small, invisible image files embedded in websites or emails that send information back to a server when loaded. These pixels allow advertisers and analytics firms to monitor user engagement, determine email open rates, and track conversions. Facebook's Pixel and Google's tracking scripts are among the most widely used, enabling companies to link browsing behavior with user profiles. The legal scrutiny of tracking pixels has intensified in recent years, particularly in cases where plaintiffs argue that pixels operate as unauthorized wiretaps by capturing users data without explicit consent. [. . .]
>
> JavaScript-based tracking scripts enable more sophisticated data collection by dynamically executing code on a webpage. These scripts can log keystrokes, track mouse movements, and capture form inputs, often relaying this data to third-party servers in real time. Session replay software, a subset of JavaScript-based tracking, records a user's interactions with a webpage, including scrolling behavior and text entry. Some courts have found that such scripts may violate wiretapping laws by intercepting communications between users and websites in real time.[11]

In re Meta Pixel Healthcare Litig. shows how sensitive information can be monetized at scale through these processes:

> Plaintiffs allege that when John Doe or any other patient of MedStar presses the login button to enter their MedStar patient portal using their username or email address and password, the Meta Pixel source code causes Doe's and all other patients' computing devices to re-direct the contents of their respective patient portal login communications to Meta and then to MedStar, rather than just to MedStar. Meta allegedly redirects the patient portal login information to itself via a "SubscribedButtonClick" transmission that includes, among other things:
>
> • The patient's identity in the form of cookies, IP address, and User-Agent identifiers;
>
> • Content of the button ("Log in");
>
> • Contents of the page from which the patient clicked to log in to the patient portal; and
>
> • Content of the page the patient will land as a result of clicking "Log in" to the patient portal.
>
> As a patient browses through the MedStar website, the Meta Pixel allegedly continues to transmit information to Meta, including information about doctors, medical conditions, and appointments associated with a patient's session.
>
> Plaintiffs assert that Meta monetizes the information that it receives through the Meta Pixel by using it to generate highly-profitable targeted advertising on- and off-Facebook. They

---

[11] David Rudolph, *Litigating Corporate Surveillance: Privacy, Autonomy, Power, and Democracy in the Courtroom* (2026), pp. 117-118.

> claim that Meta can target ad campaigns to patients based on patients' browsing behavior on their medical providers' website. Meta may, for instance, target ads to a person who has (1) used the patient portal and (2) viewed a page about a specific condition, such as cancer. *These allegations appear to be borne out by plaintiffs' expert's experiences: after Smith visited five hospital websites which employ the Meta Pixel, he allegedly received many new health-related advertisements. In particular, Smith noticed that within two hours of searching for information on ulcerative colitis on one of the hospitals' websites, he was shown an advertisement related to ulcerative colitis in his Facebook video feed*.[12]

Opponents of the bill highlight how surreptitious surveillance can serve pernicious ends:

> SB 690 would allow for an expansion of the types of harmful surveillance we've seen in the recent investigation by 404 Media that found that a data broker for eight major U.S. airlines collected travelers' domestic flight records and secretly sold access to U.S. Customs and Border Protection; and a CalMatters investigation that found California's healthcare exchange had sent private health information to LinkedIn, including whether or not a person was pregnant, blind, or transgender. **SB690 would authorize this type of surveillance and remove all liability for companies who collect, sell, and share this information without your knowledge or consent.** The proposed exemptions to our privacy rights could allow immigrants' locations to be shared with ICE, LGBTQ+ individuals to be outed or tracked, abortion seekers to be surveilled, and even lawmakers to be monitored during policy negotiations. These scenarios illustrate just some of the serious privacy threats posed by this bill.

4) **CCPA**. The CCPA, as amended by Proposition 24 in 2020, grants consumers certain rights regarding their personal information, including the right to know what information is collected and shared, request deletion, limit sharing, and to opt out of sharing (or opt in for minors under 16). The law applies only to businesses that (1) earn more than $25 million in annual revenue; (2) buy, sell, or share the personal data of 100,000 or more consumers, households, or devices annually; or (3) earn 50 percent or more of their annual revenues from selling personal information.

Proponents contend the CCPA, not CIPA, governs online business activity. Alliance for Legal Fairness writes:

> In 2018, the Legislature unanimously passed the California Consumer Privacy Act to govern how businesses collect, use, and share consumers' information for typical business activities, such as website analytics and online advertising, and created an "opt- out" consent privacy regime. The Legislature considered and declined to adopt Europe's GDPR privacy law's "opt-in" consent structure because the cumbersome requirements to click through long disclosures before visiting every website is less privacy-protective. CCPA sponsor and CalPrivacy board member Alistair MacTaggart explained that "the choice facing consumers to consent or not, was actually a false one, since most consumers would simply click 'I agree' to the request for consent."
>
> This belief was also echoed by Obama-era FTC technologist and CCPA architect Ashkan Soltani, who explained that an opt-in regime would cause "opt-in fatigue" – consumers

---

[12] *In re Meta Pixel Healthcare Litig*. (N.D.Cal. 2022) 647 F. Supp. 3d 778, 785-786.

> would simply consent to whatever the service is to get an immediate benefit, at the risk of future harms.
>
> Voters further strengthened the CCPA in 2020 through a ballot initiative that expanded consumer privacy rights, enhanced protections governing sensitive personal information, and expanded the ability for consumers to use tools to opt out of the sale or sharing of their personal information.
>
> The CCPA establishes detailed statutory requirements regulating the collection, use, and disclosure of sensitive personal information and provided consumers with tools to limit the sharing of such data. Additional, heightened protections also apply to sensitive categories of information, including immigration- and reproductive-related data, which are safeguarded under the CCPA and California's shield laws.

Opponents contend that the two bodies of law serve different, complementary purposes, and that the CCPA was not intended to override other, more privacy-protective laws.[13] Opponents also assert that the CCPA's opt-out regime is ill-equipped to address surreptitious collection of personal data by undisclosed parties.

The CCPA's regulation governing notice at collection requires that the notice be made readily available where consumers will encounter it at or before the point of collection of personal information, such as through a conspicuous link.[14] The notice must include, among other things, the purposes for which categories of personal information are collected and used, and whether each category of personal information is sold or shared.[15] With respect to third party collection of information through websites, the regulation provides:

> For purposes of giving Notice at Collection, more than one business may control the collection of a consumer's personal information, and thus, have an obligation to provide a Notice at Collection in accordance with the CCPA and these regulations. For example, a first party may allow another business, acting as a third party, to control the collection of personal information from consumers browsing the first party's website. Both the first party that allows the third parties to collect personal information via its website, as well as the third party controlling the collection of personal information, shall provide a Notice at Collection. *The first party and third parties may provide a single Notice at Collection that includes the required information about their collective information practices.*[16]

As aptly stated in Assembly Public Safety's analysis of the bill:

> . . . the first party site is not required to explain which firms or companies are operating on its sites, only that the site is selling data for "analytics" or "marketing." Most sites characterize an explanation this way*: "Marketing cookies are used to track visitors across websites. The intention is to display ads that are relevant and engaging for the individual user and thereby*

---

[13] Proposition 24 states that "in the event of a conflict with other laws and the provisions of this title, the provisions of the law that afford the greatest protection for the right of privacy for consumers shall control." (Civ. Code § 1798.175.)
[14] Cal Code Regs., tit. 11, § 7012(a), (c).
[15] *Id.* at (e).
[16] *Id.* at (g)(1), emphasis added.

> *more valuable for publishers and third party advertisers."* It does not state, *"Oracle, located at www.oracle.com, tracks your personal information for sale to other third parties, including possibly law enforcement."* That would likely get much more attention than just general notices that state a site may be tracking user information to provide *"relevant marketing information."*

If the consumer opts out, CCPA regulations require first parties to notify all third parties and forward the request to any other entity that has been provided with such information.[17] If the consumer exercises their deletion right, the first party must notify all third parties unless this proves impossible or involves disproportionate effort.[18] The real-time bidding process discussed above, which involves ad tech companies broadcasting website users' information to a network of bidders instantaneously, likely makes these provisions challenging to implement.

Oakland Privacy, in opposition, sums up the issue:

> The CCPA, as amended to become the CPRA, is entirely based on first party business behavior that consumers are aware of and can choose to opt-in or opt-out of in order to control the sale or sharing of their data with others by those businesses.
>
> This is necessary and important, but it does not address third party tracking by entities that are not the business a consumer is engaging with and who are receiving an opt-out or opt-in request. An opt-out request to say Best Buy while shopping for a television does not necessarily get to an Oracle or a Meta pixel embedded on a Best Buy website or directly onto a users device. The opt-out only controls Best Buy's behavior, not that of third parties. **The CPRA asks that Best Buy try to notify third parties of the opt-out if they are aware of those third parties, but imposes no penalties as long as they make "reasonable" efforts to do so. It does not stop the third-party behavior.**

Recent legislation addresses these concerns to a degree. In 2023, the Legislature passed the Delete Act.[19] The Act required the Privacy Agency to develop and provide, beginning January 1 of this year, a streamlined process that allows consumers to submit a request for data brokers to delete their personal information . Upon receiving such a request, the Privacy Agency is required to forward the request to all registered data brokers. The Delete Act requires data brokers to honor those requests starting August 1, 2026. Once a data broker receives the request, it has 45 days to comply. In addition, the broker is required to check every 45 days to ensure the personal information has not re-acquired.

However, the CCPA does not currently require data brokers to delete a consumer's personal information when they receive a deletion request if the information did not come directly from the consumer. SB 923 (Becker), which this Committee recently passed, seeks to close this loophole by requiring a covered business, upon request, to delete the personal information the businesses has about a consumer, regardless of whether the business received the information from the specific consumer.

---

[17] *Id.* at § 7026(f)
[18] *Id.* at § 7022(b)(3).
[19] Senate Bill 362, Chapter 709, Statutes of 2023.

Additionally, AB 566 (Lowenthal, Stats. 2025, Ch.465) requires that internet browsers include an opt-out preference signal allowing consumers interacting with CCPA-covered businesses online to automatically exercise their right to opt out of the selling and sharing of their personal information. Consumers that choose to exercise this right have a more comprehensive method of opting out. The law will take effect six months after the Privacy Agency adopts regulations. However, the law does not apply to mobile operating systems, leaving smartphones and apps out of this scheme. The Legislature may wish to consider expanding this law to ensure full coverage.

If CCPA-covered businesses fail to honor the CCPA's protections, it falls to the Attorney General and Privacy Agency to investigate and enforce violations. Unlike CIPA, the CCPA offers no direct recourse to individuals for violations.

5) **Concerns with the bill in print.** The bill in print exempts any "commercial business purpose" as defined by the California CCPA from civil and criminal liability pursuant to CIPA's prohibitions on wiretapping, eavesdropping on, or recording confidential communications, intercepting and recording cellular communications, or using a pen register or trap and trace device. "Commercial business purpose" means the processing of personal information that is either (1) subject to a consumer's opt out rights under the CCPA, or (2) performed to further a "business purpose," defined in the CCPA as:

> the use of personal information for the business' operational purposes, or other notified purposes, or for the service provider or contractor's operational purposes, as defined by regulations adopted pursuant to paragraph (10) of subdivision (a) of Section 1798.185, provided that the use of personal information shall be reasonably necessary and proportionate to achieve the purpose for which the personal information was collected or processed or for another purpose that is compatible with the context in which the personal information was collected.[20]

Among the listed purposes under the definition is:

> Providing advertising and marketing services, except for cross-context behavioral advertising, to the consumer provided that, for the purpose of advertising and marketing, a service provider or contractor shall not combine the personal information of opted-out consumers that the service provider or contractor receives from, or on behalf of, the business with personal information that the service provider or contractor receives from, or on behalf of, another person or persons or collects from its own interaction with consumers.[21]

The bill in print appears to sweep more broadly than its proponents intend. It applies to all civil and criminal violations. It is not limited to website activities; it can apply to any recordings and interceptions of individual confidential communications, as long as there is a commercial business purpose in doing so. If these acts are not clearly disclosed, it is difficult to see how a consumer would be able to meaningfully exercise their opt out rights. This could unintentionally shield wiretapping violations that involve highly offensive intrusions where website users have a

---

[20] Civ. Code § 1798.140(e).
[21] *Id.* at (e)(6). "Cross-context behavioral advertising" means the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly branded internet websites, applications, or services, other than the business, distinctly branded internet website, application, or service with which the consumer intentionally interacts. (*Id.* at (k).)

reasonable expectation of privacy. Writing in opposition, the Dolores Huerta Foundation and Consumer Federation of California, states:

> Make no mistake, if this bill becomes law as currently drafted consumers will face an assault of surreptitious recording and surveillance that will be almost without limit. The subtext of SB 690 is that if corporate giants don't like how they're being held accountable for their actions against consumers, they can merely put their giant thumb on the scale to change the rules. This is how the rule of law gets undermined. One merely needs to turn on the TV or check their mobile device (which is also surveilling you, but that's another story) or read any publication to see other aspects of this full-frontal assault on the fundamental principles of the rule of law.

Recognizing the bill in print is overly broad and may entail unintended consequences, the author has agreed to amend the bill to focus solely on the civil private right of action against private actors for violations occurring on websites. To lay the foundation for these amendments, the next section examines CIPA case law.

6) **CIPA cases**. Three statutes are at issue in the recent surge in litigation under CIPA relating to website tracking: Penal Code sections 631 (wiretapping), 632 (confidential communications), and 638.51 (pen register). The first two statutes apply to the interception of the content of communications, whereas the pen register statute applies to addressing or routing information about the communication.

Proponents of SB 690 claim that CIPA is antiquated, having only recently been stretched to apply to online communications. SB 690, as currently in print, lumps these three statutes together and, in effect, seeks to exempt all commercial online activity from their ambit. However, each statute plays a different role and involves different elements, and so should be assessed individually. Case law for each statute is discussed below.

a. Pen register cases.

Pen register claims are currently the primary vehicle for website-tracking claims under CIPA. The pen register statute is much newer than the wiretapping and confidential communications statute, which have longstanding precedents extending them to online communications. Moreover, unlike the genuine privacy violations that the other two statutes have been applied to, the purported violations of the pen register statute in this context generally appear to involve ordinary and benign operation of websites.

"A traditional phone pen register collects information about a phone call from Party A to Party B—such as the phone number called and length of the call—but does not collect the contents of what was said (which would be a wiretap). The traditional pen register will then transmit the phone number and length of call to the law enforcement officer."[22] The Federal Pen Register Act was enacted in 1986 as part of the Electronic Communications Privacy Act, in response to a United States Supreme Court ruling holding that installation and use of a pen register by police to obtain information on a suspect's telephone calls was not a "search" within the meaning of the

[22] *Vishal Shah v. Fandom, Inc*. (N.D.Cal. 2024) 754 F. Supp. 3d 924, 929.

Fourth Amendment because she "entertained no actual expectation of privacy in the phone numbers she dialed."[23]

California adopted its own version of the pen register statute in 2015 (AB 929, Chau, Stats. 2015, Ch. 204), which largely mirrors its federal analog. The statute, like the rest of CIPA, generally focuses on telephonic communications.[24] The Legislative history did not specifically address online technologies; rather, the focus was on giving guidance to law enforcement and courts for the issuance of pen register orders. However, cases had already interpreted the federal Pen Register Act to apply to internet communications.[25]

Section 638.51(a) prohibits "any person" from installing or using a pen register or a trap and trace device without first obtaining a court order. "Pen register" means "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."[26] "Trap and trace devices" are similarly defined; pen registers record information about *outgoing* communications, while trap and trace devices record information about *incoming* communications.

Pen register claims involving website activity generally assert that accessing a website is an outgoing communication; thus, when website owners install software that relays, for example, user IP addresses to third parties, the website owner has "installed" a "process" that "records" "addressing" information, thereby violating the statute.[27] There is no published California appellate authority on the application of this statute to software. Federal courts and state trial courts assessing these claims have reached very divergent results, examined in brief below.

i. Federal court cases.

The vast majority of federal district court cases in California have held that third-party collection of information about website users may constitute a pen register. In denying motions to dismiss, these courts have generally followed the reasoning of a 2023 Southern District decision, *Greenley v. Kochava*, in which the plaintiff alleged:

> Defendant was a "data broker []' that provides a software developer kit ("SDK") to software application ("app") developers "to assist them in developing their apps. In return, the app developers allow Defendant to 'surreptitiously intercept location data' from an app user ("user") via its SDK. Defendant then sells 'customized data feeds to its clients'—such as

---

[23] *Smith v. Maryland* (1979) 442 U.S. 735, 745-746.
[24] Indeed, CIPA only mentions websites in one statute, which prohibits the dissemination of confidential recordings online. (§ 632.01.)
[25] E.g. *In re United States* (D.D.C. 2006) 416 F.Supp.2d 13, 17 ("The plain language of the statute makes clear that pen registers and trap and trace devices may be processes used to obtain information about e-mail communications. The statute's history confirms this interpretation and there is no support for a contrary result.")
[26] § 638.50(b). In turn, section 629.51(a)(2) defines "[e]lectronic communication" as "any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature in whole or in part by a wire, radio, electromagnetic, photoelectric, or photo-optical system."
[27] The statute provides exceptions, including if consent has been obtained, but those exceptions apply only to "provider[s] of electronic or wire communications service." (Pen. Code § 638.51(b).) The term "electronic communication service" is not defined in CIPA, but federal law, after which much of CIPA is modeled, defines the term as "any service which provides to users thereof the ability to send or receive wire or electronic communications." (18 USC § 2510 (15).)

> Airbnb, Disney+, and Kroger—to 'assist in advertising and analyzing foot traffic at stores or other locations.' In other words, Defendant coded its SDK for data collection and embedded it in third-party apps; the SDK secretly collected app users' data; and then Defendant packaged that data and sold it to clients for advertising purposes."[28]

The court concluded that while the definition of pen register is "specific as to the type of data a pen register collects" the statute is:

> . . . vague and inclusive as to the form of the collection tool – "a device or process." [Citation.] This indicates courts should focus less on the form of the data collector and more on the result. Thus, the Court applies the plain meaning of a 'process' to the statute. A process can take many forms. Surely among them is software that identifies consumers, gathers data, and correlates that data through *unique "fingerprinting."*[29]

Relying on *Greenley*, the Northern District, in *Shah v. Fandom*,[30] denied a website operator's motion to dismiss a claim that the website's third-party tracking software constituted an unauthorized pen register.[31] The court concluded that, when the browser accesses the website, the HTTP request constituted an "electronic communication" and that the trackers' interception of IP addresses constituted the recording of "addressing" information associated with this communication.[32] The court rejected the defendant's argument that "the Trackers cannot be pen registers because the user 'necessarily and voluntarily discloses' its IP address to Fandom by visiting its website."[33] The court stated: "A user who consents to disclose their IP address to Fandom as part of accessing its website *does not necessarily consent to disclose their IP address to the third parties* operating the Trackers. The question would be 'whether the user agreed to the specific use or collection.'"[34] The court also concluded that the plaintiffs had alleged a sufficient injury for purposes of standing:

> Perhaps Plaintiffs should expect to reveal their IP addresses to the gamespot.com website, and possibly even to third parties who provide the advertisements that load when Plaintiffs visit that website. But that does not necessarily mean that Plaintiffs should reasonably expect to have Trackers installed that send their IP addresses to third parties every time Plaintiffs visit gamespot.com. *Plaintiffs have plausibly alleged that they were injured by being tracked across multiple visits for marketing and advertising purposes, and that they did not expect or agree to such tracking*.[35]

---

[28] *Greenley v. Kochava, Inc*. (S.D.Cal. 2023) 684 F. Supp. 3d 1024,1035.
[29] *Id.*, 1050, emphasis added.
[30] (N.D.Cal. 2024) 754 F.Supp.3d 924.
[31] "As is fairly routine on many websites, when users accessed the website, it would instruct trackers to be installed on the user's browser. The trackers would instruct the user's browser to send the user's IP address to third parties. The trackers would store a cookie in the user's browser cache, which the trackers would locate whenever the users returned to the website, causing their IP address to be sent to third parties each time. The third parties used this information to facilitate targeted advertising and conduct website analytics." (*Id.*, p. 931.)
[32] *Ibid.*
[33] *Ibid.*
[34] *Id.*, p. 932, emphasis added.
[35] *Ibid.*, emphasis added. See also *Fregosa v. Mashable, Inc*. (N.D.Cal. Oct. 9, 2025, No. 25-cv-01094-CRB) 2025 U.S.Dist.LEXIS 200770, at *20 ("Fregosa does not allege that Mashable violated CIPA simply by receiving IP addresses as part of an ordinary online exchange. Rather, the [complaint] alleges that Mashable affirmatively embedded third-party trackers that recorded and transmitted users' identifying information to outside entities for profiling and advertising purposes.")

The court specifically contrasted this with cases involving "situations where users were directly communicating with the party alleged to be operating the pen register and voluntarily sent that party their IP address," one of which stated that "the [federal] Pen Register Act cannot be intended to prevent individuals who receive electronic communications from recording the IP information sent to them."[36] The court concluded:

> The Court recognizes Fandom's concern that allowing this lawsuit to proceed could unsettle the basic operating rules of the Internet. It may be, as Fandom contends, that users routinely disclose their IP addresses to third parties in the process of accessing a website, and that websites sometimes do not obtain users' consent for those practices through a Privacy Policy or Terms of Use. The Court's task is to interpret the law as the Legislature wrote it. The pen register statute is broadly written, and under California law, is to be interpreted broadly to protect privacy and to be applied to new techniques and technologies. *That statute reflects the Legislature's judgment that an individual's consent is required before others may track certain addressing information in their electronic communications for non-law enforcement purposes.* To the extent that Fandom believes the statute may impose too many burdens when applied to the realities of modern technologies, and that it is too unwieldy to obtain users' consent through disclosures of the practices at issue, the question of whether the statute's scope should be narrowed ultimately rests with the Legislature, not the courts.[37]

Mirmalek v. Los Angeles Times[38] involved a similar set of facts – in fact, the *Times* website installed trackers for the same three third-party companies as in *Shah*. As in *Shah*, the plaintiff alleged the *Times'* website caused third-party trackers to be installed on website visitors' web browsers without consent, relaying their IP addresses each time they interacted with the website. Facing billions in potential damages, the *Los Angeles Times* moved to dismiss the case, arguing that the pen register statute was not intended to govern ordinary website advertising. The court relied heavily on *Shah* in denying the motion to dismiss. Several other courts have followed suit.[39]

These cases involved covert third-party tracking that intercepted communications between the user and website. By contrast, the Northern District concluded that Apple's first-party apps and their underlying processes are a part of the source of transmitted communications, as opposed to a separate process that captures metadata about those communications, and thus are not pen registers.[40]

ii. State trial court cases.

State trial courts have mostly dismissed pen register claims based on website trackers, with several courts concluding CIPA was not intended to apply to online communications. However,

---

[36] *Id.* at fn. 3, quoting *Capitol Records, Inc. v. Thomas-Rasset* (D. Minn. June 11, 2009) No. CIV 06-1497(MJD/RLE), 2009 U.S. Dist. LEXIS 50075, 2009 WL 1664468, at *3.
[37] *Id.*, pp. 932-933.
[38] (N.D.Cal. Dec. 12, 2024, No. 24-cv-01797-CRB) 2024 LX 79390.
[39] E.g. *Caldwell v. InMobi Pte., Ltd.* (N.D.Cal. Apr. 29, 2026, No. 25-cv-09977-AMO) 2026 LX 229530, at *1 (ad tech company); *Riganian v. LiveRamp Holdings, Inc*. (N.D.Cal. 2025) 791 F. Supp. 3d 1075, 1092 (data broker); *Harris v. iHeartMedia, Inc.* (N.D.Cal. Jan. 29, 2026, No. 25-cv-06038-EKL) 2026 LX 11956, at *8 (website with third-party trackers); *In re Meta Pixel Tax Filing Cases* (N.D.Cal. 2025) 793 F. Supp. 3d 1147, 1151.
[40] *In re Apple Data Priv. Litig.* (N.D.Cal. Jan. 20, 2026, No. 5:22-cv-07069-EJD) 2026 LX 32344, at *18.

as contrary published federal decisions have been handed down, some trial courts have relied on these cases in allowing pen register cases to proceed.

In *Licea v. Hickory Farms LLC*,[41] the court granted a demurrer (motion to dismiss) where the plaintiff made the bare assertion that the defendant's collection of his IP address constituted an unauthorized pen register. The court distinguished *Greenley*, finding that "nothing in the complaint establishes an IP address as equivalent to the 'unique fingerprinting' relied upon by the Southern District when finding embedded software into a mobile phone, thereby providing unique location and other information normally within the domain of law enforcement officers with a warrant."[42] The court also noted the telephonic-focus of CIPA and declined to adopt a broad interpretation of the statute, stating:

> The court also finds public policy strongly disputes Plaintiff's potential interpretation of privacy laws as one rendering every single entity voluntarily visited by a potential plaintiff, thereby providing an IP address for purposes of connecting the website, as a violator. Such a broad based interpretation would potentially disrupt a large swath of internet commerce without further refinement as the precise basis of liability, which the court declines to consider.[43]

Casillas v. Transitions Optical, Inc.[44] concluded that the contention that a website's use of a beacon to collect an IP address constituted a violation of CIPA was "merely describing what happens every time any user accesses any website. Any computer that is used to access the internet needs an IP address to do so."[45] The court stated: "The pen register statute did not, and does not, criminalize the process by which all websites communicate with all users who choose to access them."[46]

In *Sanchez v. Cars.Com Inc.*,[47] the court concluded that CIPA was inapplicable to the defendant's website's use of a beacon that collected IP address information. The court reviewed the pen register statute's legislative history and essentially drew the opposite conclusion of that in *Greenley*:

> Here, the legislative history of the CIPA suggests that "pen register" and "track and trace devices" refers to devices or processes that are used to record or decode dialing, routing, addressing, or signaling information from telephone numbers, not internet communications such as websites. Penal Code section 638.51 and its legislative history suggest that section 638.51 applies only to telephone- tracking technology, not IP address-collecting software used by a website to improve its user functionality and the effectiveness of its marketing. The California legislature enacted Assembly Bill 929, the genesis of CIPA section 638.51, in 2015 to create a comprehensive framework governing how California law enforcement officials could obtain and use a pen register or trap and trace device, just like its federal counterpart.

---

[41] 2024 Cal. Super. LEXIS 66498.
[42] *Id.* at *8.
[43] *Licea v. Hickory Farms LLC*, 2024 Cal. Super. LEXIS 66498.
[44] 2024 Cal. Super. LEXIS 70523.
[45] *Id.*, *6.
[46] *Id.*, *10. *Aviles v. Liveramp, Inc*., 2025 Cal. Super. LEXIS 776, *7 ("Without alleging that Defendant installed software on Plaintiff's device or browser that collected incoming contact information to Plaintiff's device, Plaintiff has not alleged anything above and beyond how the internet normally works.")
[47] 2025 Cal. Super. LEXIS 710.

> In enacting Assembly Bill 929, the California Legislature adopted the same authorization provision in CIPA section 638.52 that courts have relied on under the federal Pen Register Act to find that the Act applied only to mechanical, telephone number-tracing technology, not technology used to collect the IP address from a desktop computer. Thus, the legislative history of the CIPA suggests that "pen register" and "track and trace devices" refer to devices or processes that are used to record or decode dialing, routing, addressing, or signaling information from telephone numbers, and not internet communications such as websites.[48]

Rodriguez v. Ink Am. Int'l Grp. LLC,[49] in adopting similar logic, concluded that the CCPA was intended to govern such issues and that it would be rendered nugatory if CIPA applied to the conduct in question.[50]

However, some trial courts have begun following the federal courts.[51] For example, in *In re Moving Party*, in which Variety's website installed third-party trackers that relayed IP addresses and other identifiers to third parties, the court noted the number of published federal cases and found them persuasive.[52] The court also concluded that overlapping enforcement did not create a conflict between CCPA and CIPA, stating that the two bodies of law are complementary.[53] Similarly, the court in *Zhizhi Xu v. Reuters News & Media, Inc*. pointed to intent language in the CCPA requiring that it be harmonized with other privacy laws and, in the event of a conflict, that the most privacy protective laws be given effect.[54]

b. Wiretapping cases.

Unlike the pen register statute, which applies to information about communications, Section 631 prohibits surreptitious interception of the *content* of communications. Plaintiffs often plead CIPA wiretapping claims along with federal wiretapping claims; the two statutes are similar, although violations of the federal statute are harder to prove because parties to the communications can only be held liable if they intercept the communication for a criminal or tortious purpose.[55]

Section 631(a) provides, in pertinent part: "Any person who, . . . in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any . . . communication while the same is in transit or passing over any wire, line, or cable . . . is punishable [by fine or imprisonment]." The statute also punishes anyone "who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or

---

[48] *Ibid.*; see also *Rodriguez v. Ink Am. Int'l Grp. LLC*, 2025 Cal. Super. LEXIS 84257 ("CIPA's structure and history indicate that its pen-register provisions were aimed at telephonic-style surveillance, not at the routine operation of commercial websites or analytical software. As such, the statute cannot reasonably be read as broadly as Plaintiff attempts to read it.")
[49] *Rodriguez v. Ink Am. Int'l Grp. LLC*, 2025 Cal. Super. LEXIS 84257.
[50] *Id.* *10-11.
[51] E.g. *Esparza v. S&B Filters, Inc*., 2026 Cal. Super. LEXIS 13451; *Zhizhi Xu v. Reuters News & Media, Inc*., 2025 Cal. Super. LEXIS 76169; *In re Moving Party: Variety Media*, LLC 2025 Cal. Super. LEXIS 60788.
[52] *In re Moving Party: Variety Media*, LLC 2025 Cal. Super. LEXIS 60788 *3-4.
[53] *Id.*, *6.
[54] 2025 Cal. Super. LEXIS 76169 *6. ("CCPA explicitly states that 'law relating to consumers' personal information should be construed to harmonize the provisions of this title.' (See Civ. Code § 1798.175.) Moreover, it states that 'in the event of conflict between other laws and the provisions of this title, the provisions of the law that afford the *greatest protection for the right of privacy* for consumers shall control.' (*Ibid*, [emphasis added].)
[55] 18 USC 2511(2)(d).

things mentioned above in this section" – potentially putting website owners on the hook for third party trackers that have a predicate violation.

Unlike the pen register statute, it is well established that the quoted portion of the wiretapping statute applies to online communications. "Though written in terms of wiretapping, Section 631(a) applies to Internet communications."[56] Nevertheless, the statute's elements – "read," "learn," "contents," "in transit" – have led to confusion in courts.[57]

Most relevant to this bill is the meaning of "contents." According to the Ninth Circuit, the term has the same meaning as the parallel term in the federal Wiretap Act: "any information concerning the substance, purport, or meaning of that communication."[58] The term "'refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication.'"[59] As stated in *Greenley*:

> The statute does not provide clarity on the definition of "contents," and so courts have penciled in a dividing line. On one hand, courts have found that the contact information of the communicating parties and the geolocation of the communicating parties are not the "contents" of a communication under Section 631. [Citations.] On the other hand, information about particular activity conducted and search terms used on an app qualify as the "contents" of communication. [Citations.][60]

Hence, *In re Meta Pixel Healthcare Litig*., log-in buttons and descriptive URLs that contained words like "colitis" were considered content because this information was part of the substantive communications between patients healthcare websites that Meta intercepted via pixels.[61]

Recently, some judges have raised concerns about the statute's application to website tracking. In a concurring opinion written last year, Justice Bybee of the Ninth Circuit, writing about a different clause in the statute, stated:

> If the California legislature wanted to apply § 631(a) to the internet, it could do so by amending that provision or adding to CIPA's statutory scheme. Indeed, it "augmented the statutory scheme in 1985, 1990, and 1992 'to take account of privacy issues raised by the increased use of cellular and cordless telephones.'" [Citations]. For example, the California legislature added § 632.7 in 1992. That provision criminalizes nonconsensual interception and recording of "a communication transmitted between," among other things, "two cordless telephones." Cal. Penal Code § 632.7. The California legislature also added § 632.01 in 2017. That provision punishes anyone who violates § 632(a) (a section that penalizes

---

[56] *Javier v. Assur.* IQ, LLC, No. 21-16351, 2022 U.S. App. LEXIS 14951 at *1 (9th Cir. May 31, 2022); *In re Google*, 2013 U.S. Dist. LEXIS 172784, at *20 ("[T]he Court finds no reason to conclude that the limitation of 'telegraphic or telephone' on 'wire, line, cable, or instrument' in the first clause of the statute should be imported to the second clause of the statute."); *Greenley v. Kochava, Inc*. (S.D.Cal. 2023) 684 F. Supp. 3d 1024, 1051 ("courts have concluded that the first clause does not apply to internet connections, while the second clause does").
[57] See *Doe v. Eating Recovery Ctr. LLC* (N.D.Cal. 2025) 806 F. Supp. 3d 1109, 1112, 1119.
[58] 18 U.S.C. § 2510(8). See *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 607 (9th Cir. 2020).
[59] *Yoon v. Lululemon USA, Inc.* (C.D. Cal. 2021) 549 F. Supp. 3d 1073, 1082, quoting *In re Zynga Priv. Litig.*, (9th Cir. 2014) 750 F.3d 1098, 1106.
[60] *Greenley v. Kochava, Inc*. (S.D.Cal. 2023) 684 F. Supp. 3d 1024, 1051-1052, citations to plaintiff's allegations omitted.
[61] (N.D.Cal. 2022) 647 F. Supp. 3d 778, 795-796.

> eavesdropping) and then "intentionally discloses or distributes, in any manner, in any forum, including, but not limited to, Internet Web sites and social media . . . the contents of a confidential communication with a health care provider . . . ." *See* Cal. Penal Code § 632.01. California has failed to update § 631(a) to account for advances in technology since 1967. It is not our job to do it for them.[62]

Last year, in granting summary judgment for a defendant website operator, Judge Chhabria of the Northern District wrote:

> The language of CIPA is a total mess. It was a mess from the get-go, but the mess gets bigger and bigger as the world continues to change and as courts are called upon to apply CIPA's already-obtuse language to new technologies. Indeed, we have reached the point where it's often borderline impossible to determine whether a defendant's online conduct fits within the language of the statute.
>
> [. . .]
>
> As difficult as it is to apply CIPA to the physical world, it's virtually impossible to apply it to the online world. Hopefully, the Legislature will go back to the drawing board on CIPA. Indeed, it would probably be best to erase the board entirely and start writing something new. But until that happens, courts should not contort themselves to fit the type of conduct alleged in this case into the language of a 1967 criminal statute about wiretapping. Because the evidence is undisputed that Meta did not read, attempt to read, or attempt to learn the contents of Doe's communications with ERC while those communications were in transit, ERC is entitled to summary judgment on Doe's CIPA claim.[63]

On the other hand, it is worth noting that many meritorious cases can fall under this statute. Last month, for example, a court allowed a section 631 claim to proceed against Meta where it:

> allegedly developed a novel technique to transmit a unique identifier from an Android user's browser through the phone's internal simulated ports. Plaintiffs say that Meta's Android apps would listen to the communications sent through these ports and link the unique identifier with the user's Meta accounts. Through this backdoor, Meta could allegedly be assured of matching browsing activity to accounts. Though the Android operating system did not specifically block this technique, Meta's actions allegedly circumvented technical norms about sandboxing protection on Android phones. Meta allegedly evolved its technique over time to evade detection and the operating system's attempts to block it.[64]

c. Confidential recordings cases.

Section 632(a) provides: "A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device." A "confidential communication" is "any communication carried on in circumstances as may

---

[62] *Gutierrez v. Converse Inc.* (9th Cir. July 9, 2025, No. 24-4797) 2025 U.S. App. LEXIS 16844, at *5-7 (Bybee, J., concurring).
[63] *Doe v. Eating Recovery Ctr. LLC* (N.D.Cal. 2025) 806 F. Supp. 3d 1109, 1112, 1119.
[64] *In re Meta Android Priv. Litig.* (N.D.Cal. May 11, 2026, No. 25-cv-04674-RFL) 2026 LX 247754, at *7.

reasonably indicate that any party to the communication desires it to be confined to the parties thereto, . . . or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded."[65]

Courts generally presume that internet communications do not give rise to a reasonable expectation of privacy, in part because they are written communications that are by their very nature recorded and readily shareable with other recipients.[66] This has been applied to emails, chat messages, and text messages.[67] And the Ninth Circuit has noted in dicta, "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."[68] To survive a motion to dismiss, "plaintiffs must plead unique, definite circumstances rebutting California's presumption against online confidentiality."[69]

However, courts have found that the presumption does not apply where the defendant has made representations that communications will be kept private. *Brown v. Google* did not apply the presumption to Google's alleged collection of data while plaintiffs used their browsers in "private browsing mode."[70] Google had specifically indicated to users that their searches in "incognito" or "private" mode would be protected.[71] By contrast, merely alleging that a website collects search terms and other communications, without more, "does not allow the Court to infer that Plaintiff had an objectively reasonable expectation of privacy."[72]

Section 632 was the basis for liability in litigation involving the Flo App, which tracks information about women's reproductive health. Plaintiffs alleged that although Flo promised users that their sensitive health information would not be disclosed, Flo conveyed health information users entered in the app through Meta's software, enabling the companies to eavesdrop on users' private in-app communications.[73] Finding that the plaintiffs had a reasonable expectation of privacy and that Meta had intentionally eavesdropped or recorded their confidential communications without consent, the jury returned a verdict for the plaintiffs.[74]

Given the presumption that internet communications do not give rise to a reasonable expectation of privacy, section 632 seems less susceptible to abuse – and this appears to be borne out by comparatively small number of recent cases invoking this section.

d. Summary.

Claims under the pen register statute represent the bulk of the recent website-tracking litigation surge. Unlike the wiretapping and confidential recording statutes, the pen register statute is

---

[65] § 632(c).
[66] *In re Apple Data Priv. Litig*. (N.D.Cal. Jan. 20, 2026, No. 5:22-cv-07069-EJD) 2026 LX 32344, at *25 (listing cases).
[67] *United States v. Forrester* (9th Cir. 2008) 512 F.3d 500, 510; *Cline v. Reetz-Laiolo* (N.D. Cal. 2018) 329 F. Supp. 3d 1000, 1051-52; *Boulton v. Cmty.Com, Inc.* (9th Cir. Jan. 28, 2025, No. 23-3145) 2025 LX 228182, at *5.
[68] *United States v. Forrester* (9th Cir. 2008) 512 F.3d 500, 510.
[69] *Rodriguez v. Google LLC* (N.D. Cal. May 21, 2021) No. 20-cv-04688-RS, 2021 U.S. Dist. LEXIS 98074, at *7.
[70] 525 F. Supp. 3d 1049, 1055 (N.D. Cal. 2021).
[71] *Id.*, 1057.
[72] *Greenley v. Kochava, Inc., supra,* 684 F.Supp.3d at p. 1053.
[73] *Frasco v. Flo Health et al* complaint (N.D. Cal, Jun. 12, 2025) Case 3:21-cv-00757-JD.
[74] https://storage.courtlistener.com/recap/gov.uscourts.cand.372884/gov.uscourts.cand.372884.756.0_2.pdf.

relatively new and only in the last few years have plaintiffs argued the statute applies to online activities. These cases are very easy to assert, leading to serial filings by a handful of unscrupulous plaintiffs' attorneys claiming technical violations for ordinary website activity. The result has been a mess for courts, a weapon against businesses, and a seemingly unneeded tool to protect against genuine privacy violations.

Courts are split as to whether the pen register statute in fact applies to online communications. Federal courts almost uniformly conclude that it does; state courts mostly conclude the opposite. As with most of CIPA, while the statute focuses on telephonic communications, it also uses broad, technology-neutral terms. Both positions are reasonable, but the existence of cases before 2015 interpreting the federal pen register statute to apply to the online context suggests that the better interpretation is that the statute embraces online activities. Given the confusion, the ease of bringing these cases, and the sheer volume businesses are facing, swift legislative action appears necessary.

The wiretapping statute, which has been on the books since CIPA was added in 1967, has long been understood to apply to online communications. The statute has also seen a recent spike in litigation, though not to the same extent as the pen register statute. Moreover, unlike the pen register statute litigation, many of the cases involve surreptitious collection of personal or sensitive information. Still, the statute's outdated wiretapping-based terminology has created confusion for courts. Judges have called for reforms to this statute as well. Targeted legislation to ensure the statute is not susceptible to abuse appears warranted, albeit not as urgent as reform to the pen register statute.

The confidential communications statute, also added in 1967, is invoked in far fewer cases. This, too, has long been understood to apply to online eavesdropping. This may be due in part to the fact that plaintiffs face the obstacle of overcoming a presumption that internet communications are not confidential. Like the wiretapping statute, this statute has long been understood to apply to illicit recordings of online communications, which can entail egregious privacy violations – as was the case in the recent litigation in which Meta collected sensitive reproductive information from the Flo app.

Finally, it's important to note that many cases, particularly those in federal court, involve state and federal claims beyond CIPA,[75] which often survive motions to dismiss. As stated in a recent legal blog entry following a successful motion to dismiss: "With wiretapping claims losing a bit of traction in California federal and state courts of late, the plaintiffs' bar has pivoted to other privacy laws, such as California's Comprehensive Computer Data Access and Fraud Act, and the Electronic Communications Privacy Act."[76] CIPA is a focal point, but it is far from the only means of litigating over website tracking.

7) **Committee amendments.** To focus on the key driver of vexatious litigation under CIPA, the author has agreed to amend the bill to replace its contents with provisions that eliminate the private right of action under CIPA for violations of the pen register statute only. These changes

---

[75] E.g., the Wiretap Act (18 U.S.C. § 2510 et seq.), the Stored Communications Act (18 USC 2707), the California Computer Data Access and Fraud Act (Pen. Code § 502), common law invasion of privacy, and common law intrusion upon seclusion. (*See* e.g. *Brown v. Google LLC* (N.D.Cal. 2021) 525 F. Supp. 3d 1049, 1060.

[76] David Klein, "Not Going to California – Wiretap Claims Dismissed" (Jun. 15, 2026) https://kleinmoynihan.com/not-going-to-california-wiretap-claims-dismissed/.

would apply with respect to online activity by private actors only. In lieu of private enforcement, the Attorney General would have standing to pursue these pen register violations using the remedies currently provided in CIPA's right of action.

To relieve defendants in pen register lawsuits initiated before the bill becomes operative January 1, 2027, the amendments would apply retroactively to any pending litigation filed within the two-year window before January 1, 2027. The amendments would not affect any case for which a final judgment has been entered. Nor would the amendments affect claims for violations of other statutes.

Finally, a severability clause will be added in view of possible constitutional challenges to the retroactivity provisions.

As amended, the bill, in its entirety, will read:

Amendment 1: Strike all changes to sections 631, 632, 632.7, and 638.50, removing those sections from the bill.

Amendment 2*:* Change section 4 of the bill as follows:

~~**SEC. 4**~~ ***SEC. 1.*** Section 637.2 of the Penal Code is amended to read:

637.2. (a) ~~A~~ ***Except as provided in subdivision (d), a*** person who has been injured by a violation of this chapter may bring an action against the person who committed the violation for the greater of the following amounts:

(1) Five thousand dollars ($5,000) per violation.

(2) Three times the amount of actual damages, if any, sustained by the plaintiff.

(b) ~~A~~ ***Except as provided in subdivision (d), a*** person may, in accordance with Chapter 3 (commencing with Section 525) of Title 7 of Part 2 of the Code of Civil Procedure, bring an action to enjoin and restrain a violation of this chapter and may, in the same action, seek damages as provided by subdivision (a).

(c) It is not a necessary prerequisite to an action pursuant to this section that the plaintiff has suffered, or be threatened with, actual damages.

~~(d) This section does not apply to the processing of personal information for a commercial business purpose.~~

(d) (1) An action against a private actor for a violation of section 638.51 alleged to arise from conduct occurring on an internet website, online application, or mobile application may be brought under this section only by the Attorney General.

(2) The amendments to this section by Senate Bill No. 690 of the 2025-2026 Regular Session apply retroactively to any pending claim in an action commenced within two years before the operative date of that legislation.

(e) This section does not affect Title 4 (commencing with Section 3425.1) of Part 1 of Division 4 of the Civil Code.

Amendment 3: Add a new section 2 to the bill:

> ***SEC. 2. The provisions of this act are severable. If any provision of this act or its application is held invalid, that invalidity shall not affect other provisions or applications that can be given effect without the invalid provision or application.***

Going forward, the author may wish to add an urgency clause to expedite these changes.

ARGUMENTS IN SUPPORT: The Alliance for Legal Fairness writes of the bill in print:

> **Without SB 690, California businesses are caught in a legal trap**
>
> Over the past two years, a handful of trial attorneys have been misusing a 1967 criminal wiretapping statute, the California Invasion of Privacy Act (CIPA), to shakedown businesses, nonprofits, and government agencies for routine online activity.
>
> A small group of trial lawyers is alleging that typical online business activities, like web analytics or online advertising, constitute "wiretapping" or an illegal "pen register" under the wiretapping statute. They argue that businesses must get an ever-evolving version of consumer "opt-in" consent before a business can, for example, assess which pages are getting the most views, save an online shopping cart, or show an ad.
>
> **Trial lawyers are targeting entities that are too small to fight back**
>
> When this effort began in early 2025, about 600 lawsuits had been filed against California businesses. Now, just 18 months later, that number has exploded to 4,000. Tens of thousands more have received demand letters telling businesses that the mere existence of a website has triggered criminal liability and thousands (if not millions) in damages owed to individuals who: a) have not suffered any injury or harm; b) are not existing customers; and c) do not have any connection to the business at all. These bad actors are actively creating legal chaos and a cottage industry of frivolous litigation.
>
> Defendants include businesses like Howdy Plumbing and Sweet E's Bakeshop, nonprofits like the Sacramento Food Bank, healthcare providers like Southern Mono Healthcare, and even public agencies like the Metropolitan Transit Authority of Los Angeles. Trial lawyers find clusters of companies in a geographic area and then paper all of them with demand letters. In the Sacramento area, one Los Angeles law firm targeted approximately 40 plumbing and HVAC companies. The law firm is a solo practice, the plaintiff in all 40 cases is another lawyer, and neither lawyers were customers of the Sacramento companies – they simply visited websites, sent demand letters accusing these businesses of criminal conduct, and expected the businesses to settle out of fear and confusion.
>
> **Litigation exposure adds up quickly**
>
> Importantly, these lawsuits do not require any proof of actual consumer harm to proceed and include $5,000 statutory damages per violation. There is no limit to the number of lawsuits a business or nonprofit can face. Under CIPA's private right of action, organizations can face statutory damages of a minimum of $5,000 per website visit, with settlement demands

ranging from $20,000 to as high as $5 billion. Accordingly, this has created massive financial exposure to nearly every California business from a legal trap.

The combination of these factors has incentivized a small group of law firms to rely on a limited pool of repeat plaintiffs who file dozens of nearly identical cases – similar to ADA lawsuits – against the businesses and organizations that make up significant sectors of California's economy. One notable recent entrant into this feeding frenzy is a nonlawyer who has filed over 100 pro se claims in the past several months; he is a convicted felon who has served a federal sentence for extortion.

CIPA puts every organization that operates a website at risk

There is an urgent need for a policy solution. Without SB 690 nearly every organization that operates a website in California – from state agencies to small businesses to nonprofits – will be sued for engaging in "criminal activity" like collecting information like IP addresses and advertising analytics.

For example, websites maintained by the California State Assembly, Senate, and this very Committee rely on the same online tools used by impacted businesses, including transmission of IP addresses to deliver webpages and ensure functionality. If those routine communications were deemed unlawful pen register activity, California's own governmental websites would fall within the statute's criminal scope simply by operating online. Such a result yields untenable outcomes because IP address transmission and routing information are inherent to internet functionality rather than surveillance or interception.

The lawsuits target not only the front-end website operators, but also back-end companies who are the lifeblood of businesses – companies that provide payroll, shipping logistics, cybersecurity and antifraud technology, cloud storage, HR and operations, and analytics and advertising tools. It is not enough for CIPA to make clear that website operators are exempt from these lawsuits – if trial lawyers target these back-end service providers, those companies' costs will rise, and it will become infinitely more expensive for the small and medium-sized businesses to do business in California.

While current lawsuits primarily target the pen register and trap-and-trace sections, the first wave of lawsuits targeted other statutory sections, and significant numbers of the current lawsuits also target Sections 631 and 632. Reform of all of these sections is necessary.

California Consumer Privacy Act (CCPA) governs online business activity, not CIPA

In 2018, the Legislature unanimously passed the California Consumer Privacy Act to govern how businesses collect, use, and share consumers' information for typical business activities, such as website analytics and online advertising, and created an "opt- out" consent privacy regime. The Legislature considered and declined to adopt Europe's GDPR privacy law's "opt-in" consent structure because the cumbersome requirements to click through long disclosures before visiting every website is less privacy-protective. CCPA sponsor and CalPrivacy board member Alistair MacTaggart explained that "the choice facing consumers to consent or not, was actually a false one, since most consumers would simply click 'I agree' to the request for consent."

This belief was also echoed by Obama-era FTC technologist and CCPA architect Ashkan Soltani, who explained that an opt-in regime would cause "opt-in fatigue" – consumers would simply consent to whatever the service is to get an immediate benefit, at the risk of future harms.

Voters further strengthened the CCPA in 2020 through a ballot initiative that expanded consumer privacy rights, enhanced protections governing sensitive personal information, and expanded the ability for consumers to use tools to opt out of the sale or sharing of their personal information.

The CCPA establishes detailed statutory requirements regulating the collection, use, and disclosure of sensitive personal information and provided consumers with tools to limit the sharing of such data. Additional, heightened protections also apply to sensitive categories of information, including immigration- and reproductive-related data, which are safeguarded under the CCPA and California's shield laws.

Legislative history makes clear that CIPA was not intended to regulate internet activity.

For example, in 2015, the Legislature enacted AB 929 for the specific purpose of authorizing state and local law enforcement to seek court orders to use pen registers and trap-and-trace devices in telephone surveillance. AB 929's legislative history does not reference internet privacy, consumer data collection, or routine website activity. Neither consumer advocates nor the business community participated in AB 929's legislative process, because no one believed it was intended to govern all future internet activity.

Additionally, not a single mention of CIPA was made in any of the CCPA's Committee Analyses. Subsequent amendments further confirm the Legislature intended it only to apply to telephone surveillance.

Notably, Assemblymember Ed Chau, who authored AB 929, later served as the lead sponsor of the CCPA in 2018. Had AB 929 been understood to regulate routine internet data practices, the Legislature would not have needed to enact comprehensive legislation specifically governing the collection and use of personal information.

Critically, the Attorney General's office has called the opt-out "the hallmark of the CCPA." The Attorney General also has the authority to enforce CIPA but has never done so for online activity. Allowing CIPA to be misused in this manner creates regulatory uncertainty and unnecessary financial burdens for businesses already in compliance with CCPA.

CIPA lawsuits benefit trial lawyers, not plaintiffs or consumers

In a recent analysis of sixty-four healthcare-related class action CIPA lawsuits, attorneys' fees averaged over $2 million per case, while the average recovery for each class member was just $17.67.

While a small handful of firms has filed 70% of the lawsuits so far, more unscrupulous lawyers are getting in on the feeding frenzy. One solo practitioner's firm has filed 147 CIPA lawsuits just since October. Out-of-state law firms are beginning to file these claims en masse. This is going to continue unless SB 690 is enacted.

SB 690 protects privacy and fixes the legal loophole being exploited by trial lawyers

Legislative action is needed because a 1967 criminal wiretapping law is making it nearly impossible for businesses and nonprofits to comply with California's modern privacy framework. New demand letters and lawsuits are cropping up daily. Courts have also issued conflicting rulings, adding to the uncertainty.

SB 690 clarifies that CCPA-regulated activities cannot be the basis for private lawsuits under the CIPA wiretapping law. SB 690 ensures that CIPA can continue to be used as it was originally intended, in cases involving real wiretapping, without being misapplied to online activity. SB 690 gives businesses a fair chance to comply and stops the legal trap that is enriching a small number of trial lawyers.

ARGUMENTS IN OPPOSITION: A coalition of opponents writes:

SB 690 would exempt commercial business purposes from the California Invasion of Privacy Act (CIPA), fundamentally weakening one of the state's longstanding, strongest privacy and consumer protection laws. CIPA was enacted to protect Californians from all forms of unauthorized surveillance, regardless of the technology used. Courts have consistently affirmed that CIPA applies to commercial actors, including large tech companies like Google, Meta, and Oracle, when they secretly intercept and record user data without consent. SB 690's proposed "commercial business purposes" exemption would create a dangerous loophole, effectively immunizing these companies from accountability and undermining a decade of judicial interpretation.

SB 690 goes far beyond what most Californians–and most Americans–would expect or tolerate when it comes to their privacy. Everyday Californians who have done nothing more than go online could be spied on, simply because a company wants to use their information to train AI or manipulate them into buying products. SB 690 would allow our baby monitors, smart TVs, tablets, pet cameras, and other everyday devices to snoop on us, listen to our conversations, and keep tabs on our online activity, all behind our backs.

SB 690 is not a "small fix"—it's a massive carve out that opens the door for Big Tech to spy on us for just about any reason. SB 690 allows companies to use wiretaps, pen registries, and tap-and-trace surveillance for almost any reason if it can be shown to hold a commercial or business purpose.

SB 690 would allow for an expansion of the types of harmful surveillance we've seen in the recent investigation by 404 Media that found that a data broker for eight major U.S. airlines collected travelers' domestic flight records and secretly sold access to U.S. Customs and Border Protection; and a CalMatters investigation that found California's healthcare exchange had sent private health information to LinkedIn, including whether or not a person was pregnant, blind, or transgender. **SB690 would authorize this type of surveillance and remove all liability for companies who collect, sell, and share this information without your knowledge or consent.** The proposed exemptions to our privacy rights could allow immigrants' locations to be shared with ICE, LGBTQ+ individuals to be outed or tracked, abortion seekers to be surveilled, and even lawmakers to be monitored during policy

negotiations. These scenarios illustrate just some of the serious privacy threats posed by this bill.

SB 690's supporters indicate that they are trying to limit and avoid litigation from a small number of lawyers. Unfortunately, this argument is a trojan horse used to usher in a sweeping reversal of Californians rights to privacy. SB 690 would allow Big Tech and data brokers to spy on Californians' emails, searches, locations, phone calls, and private conversations without their knowledge or affirmative consent. SB 690 is fundamentally contrary to California's longstanding tradition of protecting its residents' privacy—a right that is overwhelmingly popular with Americans of all parties and political persuasions.1

SB 690 is extremely dangerous, given the surveillance and harassment of vulnerable communities taking place throughout the country, and should be rejected by this committee.

REGISTERED SUPPORT / OPPOSITION:

Support

Alliance for Legal Fairness (Sponsor)
Active Security Solutions
Advancing the Seed
Alameda County Latina Chamber of Commerce
Albany Chamber of Commerce
Alert Enterprises
Alhambra Chamber of Commerce
Allways Drops
Alpha Prime Health Insurance Solutions
American Booksellers Association
American Property Casualty Insurance Association
Amy's Roofing and Solar
Anaheim Chamber of Commerce
Antioch Ace Hardware
Apartment Owners Association of California
Association of California Healthcare Districts
Association of Corporate Counsel, San Diego Chapter
Association of Corporate Counsel, San Francisco Bay Area Chapter
Association of Corporate Counsel, Southern California Chapter
Avenue of the Arts Costa Mesa
Aviator Nation
AW Media
Azure Development
Bailey Plumbing
Barbour Painting
Bay Area Council
Bay Area Hispanic Institute for Advancement
Bay Valley Roofing
Berkeley Chamber of Commerce
Biocom
Black Business Association

Brea Chamber of Commerce
Business Inceptions, Inc.
Business Software Alliance
Cal Asian Chamber of Commerce
Calbroadband
California African American Chamber of Commerce
California Alliance of Small Business Associations
California Apartment Association
California Association for Health Services at Home
California Association of Sheet Metal & Air Conditioning Contractors National Association
California Black Chamber of Commerce
California Black Health Network
California Broadcasters Association
California Business Properties Association
California Business Roundtable
California Chamber of Commerce
California Consumer Alliance
California Consumer Defense League
California Consumer Voice
California Farm Bureau
California Fuels and Convenience Alliance
California Grocers Association
California Health Coalition Advocacy
California Hispanic Chamber of Commerce
California Hotel and Lodging Association
California League of Food Producers
California League of United Latin American Citizens (CA LULAC)
California Local Business Connection
California Manufacturers and Technology Association
California Multicultural Business Alliance
California New Car Dealers Association
California News Publishers Association
California Renewable Energy
California Restaurant Association
California Retailers Association
California Self Storage Association
California Senior Alliance
California Small Business Association
California Solar Electric Cooperative
California Solar Storage Association
California Special Districts Association
California Travel Association
Camelot Inn & Suites
Capitol Black Chamber of Commerce
Casita Coalition
CB Communications
Celibre Medical Corporation
Central Valley Business Federation
Central Valley Taxpayers Association

Chamber of Progress
Chatsworth-Porter Ranch Chamber of Commerce
Chicana Latina Foundation
Chinese Chamber of Commerce of Los Angeles
Cinema Association of California
Citizens Against Lawsuit Abuse
Civil Justice Association of California (CJAC)
Coalition INC.
Coalition of LA Probation Unions
Community Build, Inc.
Community Housing Opportunities Corporation
Community Resource Project, Inc.
Compton Chamber of Commerce
Contra Costa Climate Control
Costa Mesa Chamber of Commerce
Coyuchi
Crash Jewelry
Darrow Everett LLP
Davis Street
Deeper Signals INC.
Delta Dental of California
Demand Base
Design Snip
Dialpad
Digitalpath, INC.
Discretion Brewery LLC
Earl Skip Cooper Foundation
East Hollywood Chamber of Commerce
Ecomback
Ecommerce Innovation Alliance
Element Electric, Inc.
Elevate California
Elk Grove Plumbing, Drain, Heating and Air
EM Energy and Air
Energy Transition Collective
Fairchild Medical Center
Familias Unidas
Families United for Equity
Family Business Association of California
Feature LLC
First Response Solar
Fisher Phillips
Folsom Lake Heating & Air
Fontana Chamber of Commerce
Fresno Chamber of Commerce
Full Orbit Web and Marketing, Inc.
Fuse Service, Inc.
GoFundMe
Golden Valley Health Centers

Golden Years Policy Council
Greater Conejo Valley Chamber of Commerce
Greater High Desert Chamber of Commerce
Greater Los Angeles African American Chamber of Commerce
Greater Los Angeles Hospitality Association
Greater Ontario California
Greater Sacramento Urban League
Greater San Fernando Valley Chamber of Commerce
Greater Stockton Chamber of Commerce
Green Technical Education & Employment
Groundswell for Water & Housing Justice
Henke Foods LLC
Hispanic Chambers of Commerce San Francisco
Howdy Plumbing
HPP Cares
Imperium Global Advisors
Independent Hospitality Coalition
Independent Insurance Agents & Brokers of California, INC.
Information Technology Industry Council
Initiating Change in our Neighborhoods Community Development Corporation
Inland Empire Latino Coalition
Interactive Advertising Bureau, INC.
Internet Law Center
Internet Works
Isyanova Law PC
JCamp Consulting
Jesse Miranda Center for Hispanic Leadership
KC Sport and Entertainment
Kingston Brass, Inc.
Klinedinst PC
La Maestra Health Centers
LA South Chamber of Commerce
Latin American & Caribbean Business Chamber of Commerce
Latin Business Association
Latino Restaurant Association
Laurel Ace Hardware
Little Armenia Gateway Monument Association
Long Beach Area Chamber of Commerce
Los Angeles Area Chamber of Commerce
Los Angeles County Business Federation (BIZ-FED)
Los Angeles County Taxpayers Association
Los Angeles Latino Chamber of Commerce
Los Angeles South Chamber of Commerce
Malaga Bank
Manatt, Phelps & Phillips, Llp
Marin Ace Hardware
Marin Builders Association
Martinez Communications
MGK Risk and Insurance

Montebello Housing Development Corporation
Monument Impact
National Action Network Sacramento
National Diversity Coalition
National Federation of Independent Business (NFIB)
Netrition INC
News Media Alliance
Nicaraguan American Chamber of Commerce Northern California
Noritz America
North Orange County Chamber of Commerce
Northwest Valley Chamber of Commerce
Oakland African American Chamber of Commerce
Oakland Latino Chamber of Commerce
Oakland Vietnamese Chamber of Commerce
Oakley Ace Hardware
OMI Cultural Participation Project
Omnigro
Orange County Black Chamber of Commerce
Orange County Business Council
Orange County Hispanic Chamber of Commerce
Orange County Vietnamese American Chamber of Commerce
Pastor Tacoy Porter
Peace Officers Research Association of California (PORAC)
Peralta Hacienda Historical Park
Pittsburg Ace Hardware
Placer County Taxpayers Association
Plumbing Heating Cooling Contractors Association of California
Primal Pastures
Rad Web Marketing
Rancho Cordova Are Chamber of Commerce
RBD Communications, Inc.
Reform Cipa Coalition
Regional Cal Black Chamber of Commerce SFV
Repkord
RestoreLA-CDC
Revinate
Ribbs Plumbing & Sewer
Roberts Family Development Center
S&B Filters
Sacramento Metropolitan Chamber of Commerce
San Deigo Regional Chamber of Commerce
San Francisco African American Chamber of Commerce
San Gabriel Valley Economic Partnership
San Juan Capistrano Chamber of Commerce
Santa Ana Chamber of Commerce
Santa Barbara South Coast Chamber of Commerce
Santa Cruz Area Chamber of Commerce
Second STAR Technologies
Securities Industry and Financial Markets Association

Semillas Community Center
Silicon Valley Leadership Group
Simi Valley Chamber of Commerce
SM2 Trust
Socksmith Design
Solano Avenue Association
Solar Technologies
Southern California Black Chamber of Commerce
Spirithoods
St. Jude Neighborhood Health Centers
Standard 5&10 Ace Hardware
Stanislaus Latino Chamber of Commerce
State Privacy and Security Coalition, INC.
Stech Group
Stiles Hall
Storable, INC.
Super Brothers Plumbing Heating & Air
Superior Sensor Technology, INC.
Tahoe Mountain Sports
Tao Clean
TeamSupport
TechNet
Technology Industry Association of California (TECHCA)
TentMakers, Inc.
The Anaheim Hotel
The Bernard Johnson Group
The Karlin Law Firm Llp
The Latina Center
The Organizing Leadership Academy
The Pizza Press
The Two Hundred for Homeownership
The Westin Anaheim Resort
Time in Destiny Economic Development Corporation
Torrance Area Chamber of Commerce
Trimble
Tropicana Inn & Suites
Truity Psychometrics LLC
U.S. Chamber of Commerce
Union of American Physicians and Dentists
United Chamber of Commerce of the San Fernando Valley
United Latinos Action
Urika Center for Policy Research
Valley Industry and Commerce Association (VICA)
Vicente Le
Visit Greater Palm Springs
Visit Lodi
Visit Oceanside
Visit Yosemite/Madera County
Voler, Inc.

Wincome Hospitality
XYPlosion

Opposition

Aapis for Civic Empowerment
Access Reproductive Justice
ACLU California Action
All Family Legal
American Federation of Musicians, Local 7
American Federation of State, County and Municipal Employees (AFSCME) California
Anti Police-Terror Project
Asian Americans Advancing Justice Southern California
Asuc Sexual Violence Commission
Bayard Rustin LGBTQ Coalition
Black Women for Wellness Action Project
California Alliance for Retired Americans
California Employment Lawyers Association
California Federation of Labor Unions, Afl-cio
California Federation of Teachers Afl-cio
California Initiative for Technology and Democracy (CITED)
California Low-income Consumer Coalition
California Nurses Association
California Public Defenders Association
California School Employees Association
Center for Ai and Digital Policy (CAIDP)
Center for Democracy and Technology
Cft – a Union of Educators & Classified Professionals, Aft, Afl-cio
Church State Council
Citizens for a Better Los Angeles
Coalition for Humane Immigrant Rights (CHIRLA)
Consumer Attorneys of California
Consumer Federation of California
Consumer Reports
Courage California
Disability Rights California
Dolores Huerta Foundation
Economic Security California Action
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Freefrom
Housing and Economic Rights Advocates (HERA)
Individual- the Law Office of J.r. Howell
Indivisible Sacramento
Initiate Justice
Justice Teams Network
Justice2jobs Coalition
Kapor Center Advocacy
LA Defensa

Laane (Los Angeles Alliance for a New Economy)
LGBT Tech
National Consumer Law Center
Nextgen California
Oakland Privacy
Orange County Rapid Response Network
Pflag Sacramento
Privacy Defense Alliance
Privacy Rights Clearinghouse
Public Law Center
Rise Economy
Sacramento LGBT Community Center
Secure Justice
Service Employees International Union California
Services, Immigrant Rights and Education Network (SIREN)
Sister Warrior Freedom Coalition
Survivors + Allies
Teamsters California
Tech Oversight California
Tech Oversight Project
TechEquity Action
Techtonic Justice
The Translatin@ Coalition
Udw/afscme Local 3930
Ultraviolet Action
United Food and Commercial Workers (UFCW)
Viet Rainbow of Orange County
Warehouse Worker Resource Center
Working Partnerships USA
Youth Justice Coalition

Analysis Prepared by: Josh Tosney / P. & C.P/ (916) 319-2200