

Date of Hearing: June 17, 2026

ASSEMBLY COMMITTEE ON INSURANCE

Lisa Calderon, Chair

SB 354 (Limón) – As Amended June 11, 2026

**SENATE VOTE:** 28-10

**SUBJECT:** Insurance Information and Privacy Protection Act

**SUMMARY:** Modernizes, expands, and strengthens laws pertaining to the collection, use, and sharing of personal information in the business of insurance. Specifically, **this bill:**

- 1) Amends and expands the privacy notice required under the Insurance Information and Privacy Protection Act (IIPPA) to include, among other things, information concerning the purposes for which the consumer’s personal information will be processed, the categories of persons with whom the information may be shared, whether and where the information may be shared outside of the United States, the consumer’s consent rights with respect to the processing and sharing of their personal information, the consumer’s right to nonretaliation for exercising privacy rights, that the consumer has a right to receive notice of an adverse underwriting decision and for the decision, and additional items specified by the Insurance Commissioner (“commissioner”); and specifies the procedures for the provision of the notice.
- 2) Requires a licensee, surplus line insurer, reinsurer, or third-party-service-provider (TPSP) to provide the notices required pursuant to the bill so that the licensee, surplus line insurer, reinsurer, or TPSP reasonably expects the consumer to receive actual notice in writing, as specified.
- 3) Provides that the notice obligations imposed upon a licensee, surplus line insurer, or reinsurer may be satisfied by another licensee, surplus line insurer, reinsurer, or TPSP, as specified.
- 4) Prohibits a licensee, surplus line insurer, reinsurer, or TPSP from processing a consumer’s personal information in a manner inconsistent with the consent provided by the consumer; requires the licensee, surplus line insurer, reinsurer, or TPSP to provide a reasonable means for the consumer to provide prior, opt-in consent or to opt out, as applicable, and to maintain a written record of the consent election; and specifies the manner in which consent must be requested, or the opportunity to opt-out must be provided, as applicable, including information that must be provided in the request for consent or the opportunity to opt out.
- 5) Clarifies that a consumer does not have the ability to opt-out of processing or sharing of personal information that is reasonably necessary for the execution of an insurance transaction or when the processing is legally required.
- 6) Requires a licensee, surplus line insurer, reinsurer that uses a TPSP to prepare an investigative consumer report about a consumer in connection with an insurance transaction to include in the contract with the TPSP that the TPSP must comply with the requirements of the specified law, and may not process personal information provided to the TPSP by the licensee, surplus line insurer, or reinsurer other than to fulfill the purpose of the contract.

- 7) Makes several procedural clarification to a consumer's right to request access to, amendment of, or deletion of the consumer's personal information in possession of a licensee, surplus line insurer, reinsurer, or insurance support organization, or its TPSPs, and includes publicly available information concerning the consumer in the possession of that entity in the information to which the consumer has access, or may request to amend or delete.
- 8) Requires a licensee, surplus line insurer, reinsurer, or TPSP to provide easily accessible means for consumers to exercise their rights, and specifies means to do so, as well as prohibited practices in the provision of access to rights; and specifies that these obligations may be satisfied through substitute performance by another licensee, surplus line insurer, reinsurer, or TPSP.
- 9) Authorizes a licensee, surplus line insurer, reinsurer, or TPSP to process a consumer's personal information as is reasonably necessary and proportionate for the following purposes:
  - In connection with an insurance transaction, as defined, or provision of "value added services or benefits" in connection with an insurance transaction, as defined.
  - For compliance with legal requirements.
  - For a lienholder, mortgagee, assignee, lessor, or other person shown on the records of a licensee, surplus line insurer, or reinsurer as having a legal or beneficial interest in an insurance policy, to protect that interest, as specified.
  - To permit a party or representative of a party to a proposed or consummated sale, transfer, merger, or consolidation of all or part of the business of a licensee, surplus line insurer, or reinsurer to review the information necessary for the transaction, as specified.
  - To permit a group policyholder to report claims experience or conduct an audit of the operations or services of a licensee, surplus line insurer, or reinsurer, if the information shared is reasonably necessary for the group policyholder to make the report or conduct the audit and is not otherwise shared.
  - To permit a governmental authority to determine the consumer's eligibility for health care benefits for which the governmental authority may be liable, as specified.
- 10) Authorizes a licensee, surplus line insurer, reinsurer, or TPSP to process a consumer's personal information upon obtaining prior, opt-in consent from the consumer, as is reasonably necessary and proportionate for the following purposes:
  - In connection with the marketing of a product or service, after receiving affirmative consent from the consumer to process the consumer's information in connection with specific marketing activity to which the consumer has consented.
  - In connection with research activity, as defined, after receiving affirmative consent from the consumer to process the consumer's information in connection with specific research activity to which the consumer has consented.

- For any other purpose not enumerated, provided that the purpose has been clearly and fully disclosed to the consumer and processing is limited to the specific activity which has been disclosed and to which the consumer has consented.
- 11) Authorizes a licensee, surplus line insurer, reinsurer, or TPSP to process a consumer's personal information on an opt-out basis as is reasonably necessary and proportionate for the following purposes, provided that the consumer has been provided with notice of the processing and the consumer's ability to opt-out of the processing, a reasonable opportunity for the consumer to opt-out of the processing, and the consumer has not done so:
- In connection with the joint marketing of cobranded financial products or services between a licensee and a financial institution, as specified.
  - In connection with cross-marketing of insurance or financial products or services, provided by either the licensee or a third party, to a consumer with which the licensee has an ongoing business relationship, if the consumer is provided with notice and the ability to opt out of the cross-marketing activity and has not done so.
  - In connection with the sharing of personal information, other than a consumer report, with an affiliate of the licensee for any purpose not specified as permissive pursuant to 9), provided that the consumer is given notice and the ability to opt out of the affiliate sharing activity.
  - In connection with FAIR Plan clearinghouse activities, as specified.
  - For additional purposes specified by the commissioner in regulation.
- 12) Prohibits a licensee, surplus line insurer, reinsurer, or third party service provider from processing a consumer's sensitive personal information, other than in connection with an insurance transaction.
- 13) Prohibits a licensee, surplus line insurer, reinsurer or TPSP from selling a consumer's personal information for any type of monetary or other valuable consideration.
- 14) Specifies that a licensee's, surplus line insurer's, or reinsurer's retention of a consumer's personal information shall be reasonably necessary and proportionate in connection with the specified purpose.
- 15) Requires a licensee, surplus line insurer, or reinsurer to develop a written records retention policy and records retention schedule and shall make it available to the commissioner upon request.
- 16) Requires a licensee to review and update its records retention policy and records retention schedule not less than once every three years to ensure compliance; requires a licensee to review its records containing personal information to determine whether any specified purposes permit the continuing retention of any consumer's personal information; and requires them to take reasonable steps to securely destroy, delete, or deidentify the consumer's personal information in a timely manner in accordance with its records retention schedule once they have determined that a consumer's personal information, or a specific

element of the consumer's personal information, is no longer needed pursuant to the specified purpose.

- 17) Requires a licensee, surplus line insurer, or reinsurer to exercise due diligence in selecting and overseeing its TPSPs; and requires them to develop written procedures for the selection and oversight of TPSPs that are to be made available to the commissioner upon request.
- 18) Requires that a contract between a licensee, surplus line insurer, or reinsurer, and a TPSP govern the processing of personal information performed on their behalf, and that the contract contain clear instructions for processing personal information, the nature and purpose of processing, the types of personal information subject to processing, the duration of processing, and the rights and obligations of all parties, as specified.
- 19) Requires a licensee, surplus line insurer, or reinsurer to develop, implement, and maintain a program of administrative, technical, and physical safeguards sufficient to ensure the confidentiality, integrity, and availability of nonpublic information in the possession of the licensee, surplus line insurer, or reinsurer.
- 20) Requires a licensee, surplus line insurer, reinsurer, or TPSP to promptly provide notice to the commissioner of an incident constituting a breach, as specified.
- 21) Requires a licensee, surplus line insurer, reinsurer, or TPSP that, pursuant to an insurance transaction, takes title to a device storing personal information of a consumer, to use commercially reasonable efforts to delete the consumer's personal information within a reasonable period of time, and shall not further process or share personal information obtained in this manner, as specified.
- 22) Prohibits retaliation against a consumer for the exercise of rights pursuant to the IIPPA.
- 23) Increases penalties for knowing and willful violations of the provisions of the IIPPA.
- 24) Provides several rights and authorities to the commissioner to enforce, and clarify through regulations and rulemaking, the provisions of the bill.
- 25) Provides that the provisions of the IIPPA as amended preempt and supersede all state laws and portions of state laws relating to consumer privacy that are inconsistent with the bill.
- 26) Makes conforming and technical changes to existing provisions of the IIPPA.
- 27) Defines various terms.

**EXISTING LAW:**

- 1) Establishes the IIPPA, which, among other things: requires insurance institutions and agents in the business of insurance to provide specified notices of information practices to all applicants and policyholders in connection with an insurance transaction; requires a disclosure authorization form meeting certain specifications to authorize the disclosure of personal or privileged information about an individual to an insurance institution, agent, or insurance-support organization; provides the rights to access, amend/correct, and delete personal information about the individual in the possession of an insurance institution, agent, or insurance support organization, pursuant to a written request, as specified; and requires

insurers to provide notice of an adverse underwriting decision to an individual that includes the reason for the decision, including the specific items of personal or privileged information that support those reasons, as specified, and limits the reason for which and adverse underwriting decision can be issued. (Insurance (Ins.) Code Sec. 791, *et seq.*)

- 2) Establishes the California Consumer Privacy Act (CCPA), which grants consumers certain rights with regard to their personal information collected by businesses, including enhanced notice, access, and disclosure; the right to deletion; the right to opt out of the sale of personal information; and protection from discrimination for exercising these rights. (Civil (Civ.) Code Section 1798.100, *et seq.*)
- 3) Establishes the California Privacy Protection Agency (CPPA) with the authority to oversee the implementation and enforcement of the CCPA. (Civ. Code Sec. 1798.199.10(a))
- 4) Directs the CPPA to adopt regulations to further the purposes of the CCPA, including, but not limited to reviewing existing Insurance Code provisions and regulations relating to consumer privacy to determine whether any provisions of the Insurance Code provide greater protection to consumers than the provisions of the CCPA; and, upon completing its review, requires the CPPA to adopt regulations that apply only the more protective provisions of the CCPA to insurance companies.(Civ. Code Sec. 1798.185(a)(20).)
- 5) Permits amendment of the CCPA by a majority vote of each house of the Legislature and the signature of the Governor, provided such amendments are consistent with and further the purpose and intent of this act as set forth therein. (Proposition 24 Sec. 25 (2020))

**FISCAL EFFECT:** Unknown.

**COMMENTS:**

- 1) *Purpose.* According to the author:

Californians are required by law to purchase many types of insurance, such as automobile, health, and workers' compensation insurance. As such, insurance companies collect significant amounts of consumer personal information. Moder-day innovations and the evolving business landscape of the insurance industry has outpaced existing insurance privacy laws. SB 354 strengthens privacy protections and ensures insurers operate under standards that protect consumer privacy from situations such as institutionalized hacking or bad actors. This bill will also give consumers information on the categories of personal information being processed, how it is collected, and with whom it is shared.

This bill is sponsored by Insurance Commissioner Ricardo Lara.

- 2) *Double referral.* This bill is double-referred to the Assembly Committee on Privacy & Consumer Protection. Should it pass out of this committee, the privacy implications of the bill will be evaluated in detail by that committee pursuant to its jurisdiction.
- 3) *IIPPA, CCPA, and Proposition 24.* Since 1981, the privacy of personal information collected, used, and shared in the business of insurance has been regulated by the Insurance Information and Privacy Protection Act (IIPPA).

The IIPPA, among other things: requires insurance institutions and agents in the business of insurance to provide specified notices of information practices to all applicants and policyholders in connection with an insurance transaction; requires a disclosure authorization form meeting certain specifications to authorize the disclosure of personal or privileged information about an individual to an insurance institution, agent, or insurance-support organization; provides the rights to access, amend/correct, and delete personal information about the individual in the possession of an insurance institution, agent, or insurance support organization, pursuant to a written request, as specified; and requires insurers to provide notice of an adverse underwriting decision to an individual that includes the reason for the decision, including the specific items of personal or privileged information that support those reasons, as specified, and limits the reason for which and adverse underwriting decision can be issued.

The IIPPA also prohibits an insurance institution, agent, or insurance-support organization from disclosing any personal or privileged information about an individual collected or received in connection with an insurance transaction, unless the disclosure is subject to the written authorization of the individual, is reasonably necessary to perform a business, professional, or insurance function and is not further disclosed, is reasonably necessary to prevent fraud or criminal activity, is permitted or required by law, is made for the purpose of conducting actuarial or research studies, as specified, is only used in connection with the marketing of a product or service provided the opportunity to opt out of that use and has given no such indication, or is used for another of a small number of specified purposes. The IIPPA also gives the commissioner the authority to prosecute violations of these provisions, and specifies the process for bringing such an action, including associated penalties.

In 2018, the Legislature passed, and Governor Newsom signed into law, the CCPA, which provides baseline privacy rights for consumer personal information maintained or transacted by businesses. The CCPA was the result of extensive negotiation among stakeholders, and was developed in part to provide a legislative path as an alternative to a ballot measure that would have otherwise moved forward. The CCPA was the first general data privacy law of its kind in the nation. In 2020, voters passed Proposition 24, the California Privacy Rights Act, which expanded and amended CCPA, and created the California Privacy Protection Agency (CPPA) as a regulatory authority to oversee its implementation and enforcement. Proposition 24 was purportedly proposed in part in response to various legislative attempts to weaken the privacy protections pursuant to CCPA. (Note: for purposes of clarity and concision, all provisions of the California Privacy Rights Act will be included in references to CCPA, unless otherwise specified.)

CCPA, as amended by Proposition 24, requires businesses to provide certain information in their privacy policies pertaining to the categories of personal information they collect, use and disclose. It also provides consumers with the right to opt out of the sale of their personal information, and to direct a business to limit the collection and use of their sensitive personal information to that which is reasonably necessary and proportionate to what an average consumer would expect in the course of the business transaction. CCPA similarly provides rights to request access, amendment, or deletion of consumer information maintained by businesses.

Section 1798.185 of the Civil Code, enacted by Proposition 24, tasks the Attorney General, and later the newly created CPPA, with promulgating regulations for a number of specified reasons critical to the implementation of the CCPA. Section 1798.185(a)(21) reads:

[On or before July 1, 2020, the Attorney General shall solicit broad public participation and adopt regulations to further the purposes of this title, including, but not limited to] review existing Insurance Code provisions and regulations relating to consumer privacy, except those relating to insurance rates or pricing, to determine whether any provisions of the Insurance Code provide greater protection to consumers than the provisions of [the CCPA]. Upon completing its review, the [CPPA] shall adopt a regulation that applies only the more protective provisions of this title to insurance companies. For the purpose of clarity, the Insurance Commissioner shall have jurisdiction over insurance rates and pricing.

Proposition 24 also provided that this regulatory authority be transferred to CPPA once the agency was established and prepared to take on regulatory responsibilities. The result of the directive in Section 1798.185(a)(21), however, is an inevitable patchwork of jurisdiction, whereby the Insurance Commissioner maintains jurisdiction over data privacy in the insurance industry for circumstances where the Insurance Code provides stronger protections for consumers, while the CPPA maintains jurisdiction over other aspects of data privacy in the insurance industry to the extent provisions of CCPA are adopted as stronger than their counterparts in the Insurance Code. Regulatory and enforcement authority are consequently split between the CPPA and the Insurance Commissioner, and compliance is exceedingly complex.

This bill seeks to more clearly establish the general jurisdiction of the Insurance Commissioner over data privacy rights of insurance consumers. Toward this end, the bill explicitly establishes that its provisions preempt and supersede all state laws and portions of state laws relating to consumer privacy that are inconsistent with the bill's provisions, except with respect to protected health information. Consistent with the intent of Proposition 24 and Section 1798.185(a)(21), the bill also establishes privacy protections for personal information processed in the business of insurance that uniformly exceed the more general privacy protections provided by CCPA.

- 4) *Sensitivity and complexity of the insurance industry.* This bill raises two fundamental questions with respect to the insurance industry: 1) is personal information exchanged in the business of insurance inherently more sensitive than information exchanged in more general contexts? And 2) can the mechanics of the insurance industry tolerate robust constraints on the collection, use, and sharing of personal information?

With several enumerated exceptions, CCPA provides data privacy protections intended to span consumer-facing industries. This includes everything ranging from online shopping to social media. Still, California law recognizes various circumstances in which the exchange of personal information is considered more sensitive, either by virtue of the specific information exchanged, or by virtue of the context in which that information exchange occurs. For instance, California provides more stringent protections for personal information in medical contexts pursuant to the Confidentiality of Medical Information Act (CMIA), in financial contexts pursuant to the California Financial Information Privacy Act (CalFIPA), and in online educational contexts pursuant to the Student Online Personal Information

Protection Act (SOPIPA). While these laws generally preceded CCPA, CCPA did not seek to supersede them, instead maintaining baseline privacy protections for consumer personal information through CCPA and guaranteeing more robust protections in these more sensitive contexts.

California also provides privacy protections beyond those offered by CCPA for certain consumer industries, including laws regulating data collected by in-vehicle cameras in motor vehicles and laws limiting the processing of genetic information by direct-to-consumer genetic testing companies. These laws came into effect after the passage of CCPA, indicating the continued intent of the Legislature to impose more restrictive privacy protections on consumer-facing industries considered particularly sensitive.

Insurance Commissioner Ricardo Lara, who sponsors the bill, argues:

More than almost any industry, insurance companies require significant amounts of personal information from consumers in order to properly manage risks. As innovative technologies and business practices continue to redefine the insurance market, California's decades-old insurance legacy laws have been outpaced by the scale, speed, and manner in which consumer personal information is processed. The significant gap in oversight concerning the use of sophisticated technologies and increasingly complex contractual arrangements between insurers and service providers leaves consumers vulnerable. Personal information is over collected, sold, and shared with entities not contemplated by the consumer, and fraud arising from data breaches has proliferated with the unauthorized exposure of consumers' personal information. The latest string of data breach incidents involving insurers continues to demonstrate how consumers' sensitive personal information is a prime target, especially among data-rich industries such as insurance.

In many cases, such as home, auto, and health insurance, insurance is either legally required or effectively essential for consumers, meaning the exchange of personal information is not elective. Insurance also tends to cover the things most dear, and therefore worthy of additional security, to the consumer, such as their life, livelihood, health, home, and valuable property. Accordingly, the process of transacting insurance can reveal intimate details of the daily lives of consumers, and the context of insurance inherently relies on a level of trust between the consumer and the licensee that arguably instills greater sensitivity than a typical consumer transaction.

On the other hand, as the Insurance Commissioner points out, the insurance industry relies heavily on the collection and evaluation of personal information to accurately price risk. This means constraints on the collection, use, and sharing of personal information have the potential to materially impact the functioning of the insurance market. The practical realities of an insurance transaction, from the consumer seeking coverage to the insurer writing a policy to the filing of claims, require personal information to be shared between various parties with relative efficiency. A typical insurance transaction from the solicitation of coverage to the processing of a claim can include the consumer, the insurance company, the agent or broker, a potential wholesaler, one or many claims adjusters, third-party service providers who process information on behalf of any of these parties, and regulatory agencies that broadly oversee the entire process. Disruptions to the transfer of information in this process can delay the placement of coverage, increase frictional costs (thereby increasing

premiums), and impede timely handling of claims, which, if unduly delayed, can significantly burden the consumer.

Many consumers also work with a preferred agent or broker over several years when seeking insurance, and the ability of that agent or broker to meet their insurance needs depends on the maintenance of personal information about the consumer for the duration of their ongoing business relationship. Insurance frequently tends to be associated with ancillary products, such as financial products that may appropriately bundle with life insurance products to better support the needs of the consumer. Agents and brokers may direct consumers toward these products based on the personal information they maintain, as appropriate, which can often be provided by affiliates or partnering entities of insurers.

The data-rich nature of the insurance industry creates conditions that are arguably more sensitive than a typical consumer transaction, while the complexity of insurance products and the associated transactions means disruptions to the efficient flow of information for purposes desired by the consumer can be costly in both time and money. A law broadly governing the processing of personal information in the insurance industry must acknowledge and balance both of these realities.

- 5) *Major distinctions between this bill and CCPA.* Both this bill and CCPA require specified privacy notices, provide rights to access, correct or amend, and delete personal information maintained by a business, and prohibit retaliation for exercise of rights, among other things. However, this bill would provide more robust constraints on the collection, use, and disclosure of personal information that is processed in the business of insurance. Major distinctions between the privacy rights provided by CCPA and this bill include the following:

Processing: The CCPA does not place specific restrictions on the collection and use of personal information, but provides consumers with the right to direct a business that collects *sensitive* personal information, as defined, to limit its use of the consumer's sensitive personal information "to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services," and as otherwise specified.

The provisions of this bill almost entirely pertain to the *processing* of personal information, which is defined to mean "any operation or set of operations performed by a licensee, reinsurer, surplus line insurer, or third-party service provider, by manual or automated means, on the personal information or sets of personal information of a consumer, including the collection, use, sharing, storage, disclosure, analysis, deletion, retention, or modification of personal information." In other words, collection, use, and sharing are all largely regulated in the same manner in this bill, as further discussed below.

Data minimization and opt-in default: The CCPA does not explicitly require minimization of data collected, used, or shared, apart from the opportunity to opt out of the sale and sharing of personal information, subject to specified exceptions. However, CCPA does provide the consumer to direct a business that collects *sensitive* personal information about the consumer to limit its use of the consumer's sensitive personal information to "that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services."

This bill places similar limitations on *all* personal information processed in the business of insurance, but limits the “necessary and proportionate” standard to only specified purposes, some of which are permissible use, and some of which are subject to opt-out standards. For any purpose that is not specifically enumerated, this bill would require opt-in consent for collection, use, and sharing of that information. In other words, while CCPA defaults to permitting the sale or sharing of personal information subject to the opportunity to *opt-out*, this bill would default to prohibiting the processing of personal information, and would require affirmative consent to do so, except as specified. This bill also prohibits the sale of personal information entirely, and addresses the sharing of personal information in largely the same manner as it addresses processing generally.

Small business exemption: The CCPA exempts from its provision any business that had annual gross revenues of less than \$25 million in the preceding calendar year, annually buys, sells, or shares personal information of fewer than 100,000 consumers or households, *and* derives less than 50% of its annual revenues from the selling or sharing of consumers’ personal information.

This bill does not provide a similar exemption for small businesses. That said, most small business that would fall under this bill are independent agencies, which may be covered by amendments recommended by the committee to address the application of the bill to producers. (See Comment #6).

Private right of action: The CCPA provides a limited private right of action that applies only to those whose personal information was subject to a data breach.

The existing IIPPA provides a private right of action with respect to the rights to access, amend/correct, and delete personal information held by an insurer, agent, or insurance support organization, and with respect to requirements pertaining to notice of adverse underwriting decisions. The bill in print expands this private right of action to include violations of restrictions on the processing of personal information including consent procedures, prohibitions on sale of personal information, retention and deletion requirements including development and reporting of a record retention policy and schedule, existing provisions pertaining to adverse underwriting decisions not currently covered by the existing private right of action, existing procedures for health insurers to protect the confidentiality of medical information that are not currently covered by the existing private right of action, and prohibitions against retaliation for exercising rights, as specified.

- 6) *Significant outstanding issues*. The bill in print poses several practical and technical issues for the business of insurance that could impact the efficient operation of the market. Key remaining issues that the author may wish to address should this bill move forward include the following:

Burden on producers: The major provisions of this bill as it is currently in print apply to all licensees, among others, which includes both insurers and producers. Producers, as defined in the bill, include several types of agents and brokers, who serve as intermediaries with the objective of connecting consumers with appropriate insurance products. Even among agents and brokers, several unique models exist; for instance, captive agents are compensated by an insurer to sell products only from that insurer, independent agents receive commission from several companies to sell products from multiple insurers, and brokers generally work on behalf of the consumer to find the optimal price and coverage among several insurers.

A coalition of organizations representing producers comprised of the Independent Agents and Brokers of California, the California Insurance Wholesalers Association, the National Association of Insurance & Financial Advisors of California, American Agents Alliance, and California Agents and Health Insurance Professionals, argues in opposition to the bill:

The CCPA was designed to address business models that monetize personal information or use it to target consumers through extensive data collection and tracking. Independent insurance agents, brokers, and wholesalers (collectively referred to as “producers”) operate very differently. They do not sell or broadly share the personal information that clients provide except when necessary to complete the insurance transactions the consumer requests. They also have strong incentives to safeguard client information because those relationships are central to the value of their businesses.

The central problem with SB 354 for independent producers is that it is aimed primarily at the information practices of large multistate and multinational insurance companies. By placing both insurers and producers within the same definition of “Licensee,” the bill imposes the same obligations and costs on a small local agency as on a global insurance enterprise. [...] Applied to independent producers, these requirements would make every client relationship significantly more burdensome by requiring layered notices, documented consent, annual rights reminders, data inventories, vendor oversight, and audit trails. [...]

Independent insurance producers do not sell customer information or solicit clients for purposes unrelated to the insurance products and services that meet their needs. They do not process, share, or sell personal information except to the extent necessary to carry out insurance transactions and fulfill their duty to protect their clients’ financial interests.

Should this bill move forward, the author may wish to consider steps to reduce the burden on producers to the extent they do not process personal information outside of a consumer’s request to solicit, obtain, or place insurance coverage.

Compliance obligations of TPSPs: The IIPPA currently applies to insurers, agents, and insurance support organizations, which are a fairly circumscribed set of organizations that collect personal information primarily to provide that information to insurance institutions or agents for insurance transactions. This typically takes the form of the compilation and/or furnishing of consumer reports, or the collection of personal information for detecting and preventing fraud and other malfeasance. This bill introduces to insurance privacy laws the concept of a TPSP, which generally includes any person that contracts with a licensee, surplus line insurer, or reinsurer, that provides services to that entity, and processes, shares, or otherwise is permitted access to personal information through its provision of services to that entity, and includes insurance support organizations. Under the bill, TPSPs that process consumer personal information are obligated to comply with the obligations it imposes, and licensees, surplus line insurers, and reinsurers are required to oversee that compliance through contractual obligations.

A coalition of business and technology aligned organizations consisting of the California Chamber of Commerce (CalChamber), CTIA, the Software Information Industry Association, TechCA, TechNet, and the American Council of Life Insurers, argues in opposition to the bill:

While our members take no issue with efforts to update existing laws to bring them into alignment with privacy rights obligations under CCPA as amended by the voters in Proposition 24 of 2020, **SB 354** fails to recognize the practical reality that businesses provide information services across industries *simultaneously* including the banking, healthcare, and government sectors – in addition to the insurance industry. Given the broad scoping changes sought by **SB 354** to amend the IIPPA to include data elements that overlap with those already defined as personal information outside of the IIPPA, it is critical that **SB 354** incorporate clear delineations regarding statutory jurisdiction within the IIPPA itself to ensure that the bill is enforceable in a manner that protects consumer privacy while avoiding undue compliance risk arising from conflicting obligations for businesses subject to regulation by the California Consumer Privacy Protection Agency (CPPA), the agency created and charged with implementing the CCPA under Prop 24.

The bill in print provides some clarity here in Section 791.39, where it specifies that “[t]his article preempts and supersedes all state laws and portions of state laws relating to consumer privacy that are inconsistent with this article.” It also clarifies that “[t]his article does not preempt or supersede existing federal or state law related to protected health information.” However, because this bill’s applicability is based on the nature of the *entity* rather than the information it is handling, it is unclear in the bill in print whether a TPSP that handles personal information from a variety of sources, including licensees, is required to comply with the bill’s provisions *with respect to information that did not originate from a licensee subject to the bill*.

Potential conflicts between parallel regulations for CCPA and IIPPA: Related to the concern raised by the aforementioned opponents is that entities governed by both CCPA and IIPPA for different information could be forced to comply with regulations governing identical terms and concepts, but with differing definitions or procedures. This can create significant confusion and hinder effective compliance.

For example, both CCPA and this bill define the term “dark pattern” to mean “a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice.” However, CCPA appends to the end of that definition “as further defined by regulation.” Regulations promulgated by CPPA in accordance with that provision are critical to laying out the contours of the definition, but would not be applicable to the identical definition of the term used in this bill, since the bill expressly indicates that “the Insurance Commissioner shall retain primary responsibility for regulation of insurance privacy practices” (Sec. 791.39(c)) and assigns the Commissioner the authority to “issue rules, regulations, and orders as the commissioner deems necessary to carry out” the bill’s provision. (Sec. 791.40)

To avoid conflicting regulations with respect to overlapping terms and concepts between CCPA and this bill, should this bill move forward, the author may wish to consider clarifying the need for compatibility between CCPA and IIPPA regulations pertaining to overlapping concepts and terms.

Scope of the private right of action: Existing law pursuant to the IIPPA provides a limited private right of action to allow any person whose rights have been violated by a violation of its provisions to seek equitable relief in any court of competent jurisdiction. This private right of action extends to the provisions of the IIPPA that pertain to the rights to access,

correct/amend, and delete personal information held by an insurer, agent, or insurance support organization.

This bill, as it is currently in print, would significantly expand the scope of the private right of action to include violations of restrictions on the processing of personal information including consent procedures, prohibitions on sale of personal information, retention and deletion requirements including development and reporting of a record retention policy and schedule, existing provisions pertaining to adverse underwriting decisions not currently covered by the existing private right of action, existing procedures for health insurers to protect the confidentiality of medical information that are not currently covered by the existing private right of action, and prohibitions against retaliation for exercising rights, as specified.

A coalition of organizations representing insurers, reinsurers, legal advocates argues in opposition to the bill:

SB 354 expands the PRA in IIPPA to cover not only a consumer's rights, but also the notices provisions of the bill. Management of notices has always been done through administrative oversight within the CDI. Subjecting errors on a disclosure form to a private right of action opens up the risk of increased litigation, which is costly to the insurer as well as the courts.

Given the complexity and broadened scope of the IIPPA as it is proposed to be amended by this bill, this expansion of the private right of action has the potential to expose a wide range of parties to liability for minor, procedural violations even when the rights of consumers are not meaningfully infringed. While larger insurers may have the capacity to challenge these lawsuits, smaller licensees such as independent brokerages may face increased litigation costs and be forced to settle potential lawsuits rather than withstand the ballooning costs of an extended legal battle.

Where a private right of action is not available, provisions of the Insurance Code have nonetheless been robustly enforced by the Insurance Commissioner where the rights of consumers have been egregiously violated. Should this bill move forward, the author may wish to consider narrowing the scope of the private right of action in the bill to ensure consumers who have had their rights violated by a licensee or TPSP have access to legal recourse without expanding frictional costs associated with litigation.

Exemption of regulations from the Administrative Procedure Act: The California Administrative Procedure Act governs the development and implementation of rules and regulations by state agencies, ensuring the opportunity for public engagement and clarity and legal validity in the resulting rules and regulations. This bill provides the Insurance Commissioner with the authority to issue rules, regulations, and orders as necessary to carry out the bill's provisions, but exempts this process from the requirements of the Administrative Procedure Act.

No compelling policy justification has been provided for this exemption, and public participation and clarity in the rulemaking process are critical for ensuring that this consumer-focused bill is implemented in accordance with the goal of protecting the privacy and agency of consumers while allowing for a robust insurance market that affordably meets consumer needs.

Categories of marketing subject to opt-out are undefined: The bill in print explicitly specifies processing of consumer personal information “in connection with *cross-marketing* of insurance or financial products [...] to a consumer with which the licensee has an ongoing business relationship” and “in connection with the *joint marketing* of cobranded financial products or services between a licensee and a financial institution,” as specified, are subject to an opt-out structure rather than opt-in affirmative consent.

However, the terms “cross-marketing” and “joint marketing” are not defined in the bill, and more general marketing purposes require opt-in consent, so the scope of marketing encompassed by these provisions is not clear. Depending on how these terms are defined, it is possible that the consent required for insurers to market their own insurance products may be more robust than the consent required for insurers to market another entity’s products or products cobranded with another entity. Ambiguity of these terms may pose compliance complications.

## **REGISTERED SUPPORT / OPPOSITION:**

### **Support**

Ahavahprem Software Corp  
Consumer Federation of California  
Department of Insurance  
Insurance Commissioner Ricardo Lara / California Department of Insurance  
Oakland Privacy  
Poindexter Consulting Group  
Privacy Defense Alliance  
Privacy Rights Clearinghouse  
Veterans in Business Network (VIB)

### **Support If Amended**

California Insurance Wholesalers Association  
The Council of Insurance Agents & Brokers  
Wholesale and Specialty Insurance Association

### **Oppose**

Copart INC.  
The Western Insurance Agents Association (WIAA)

### **Oppose Unless Amended**

American Agents Alliance  
American Council of Life Insurers  
American Property Casualty Insurance Association  
Association of California Life and Health Insurance Companies  
Building Owners and Managers Association of California  
California Agents and Health Insurance Professionals  
California Association of Realtors  
California Bankers Association

California Building Industry Association  
California Business Properties Association  
California Chamber of Commerce  
California Credit Union League  
California Escrow Association  
California Land Title Association  
California Mortgage Bankers Association  
Civil Justice Association of California (CJAC)  
Commercial Real Estate Development Association, Naiop of California  
Consumer Credit Industry Association  
Consumer Data Industry Association  
Cspra  
CTIA  
Independent Insurance Agents & Brokers of California, INC.  
Insurance Services Office, INC.  
Insured Retirement Institute  
National Association of Insurance and Financial Advisors - California  
National Association of Mutual Insurance Companies  
Pacific Association of Domestic Insurance Companies  
Personal Insurance Federation of California  
Reinsurance Association of America  
Relx INC. and its Subsidiaries  
Responsible Data Alliance (RDA)  
Software Information Industry Association  
Techca  
Technet  
The Committee of Annuity Insurers

**Analysis Prepared by:** Landon Klein / INS. / (916) 319-2086