Date of Hearing: July 1, 2026
Fiscal: Yes

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Rebecca Bauer-Kahan, Chair
SB 354 (Limón) – As Amended June 26, 2026

SENATE VOTE: 28-10

SUBJECT: Insurance Information and Privacy Protection Act

SYNOPSIS

Among the provisions of the California Consumer Privacy Act (CCPA), section 1798.185 of the Civil Code, updated by Proposition 24, tasks the Attorney General, and later the newly created California Privacy Protection Agency (Privacy Agency), with promulgating regulations for several specified reasons critical to the implementation of the CCPA. As it relates to the Insurance Information and Privacy Protection Act (IIPPA), 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 [Privacy Agency] 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 the Privacy Agency 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 Privacy Agency maintains jurisdiction over other aspects of data privacy in the insurance industry to the extent provisions of CCPA are stronger than their counterparts in the Insurance Code. As a result, regulatory and enforcement authority are split between the Privacy Agency and the Insurance Commissioner, and compliance is exceedingly complex.

This bill seeks to establish an updated privacy framework for insurance consumers to reflect advances in technology since the passage of the IIPPA in 1981, and to ensure that the IIPPA is more privacy protective than the CCPA in order to make it clear that the Insurance Commissioner has sole responsibility for regulating insurance.

This bill is sponsored by Insurance Commissioner Ricardo Lara and is supported by Privacy Rights Clearinghouse, Oakland Privacy, and the Consumer Federation of California, among others. The previous version of the bill was opposed by several insurance industry associations, the California Chamber of Commerce, and the Consumer Data Industry Association, among others. However, the June 26th amendments addressed concerns raised by some of the opposition and may move some groups to a neutral position.

This bill was previously heard by the Insurance Committee, where it passed on an 11-3 vote.

EXISTING LAW:

1) Provides, pursuant to the California Constitution, that all people have inalienable rights, including the right to pursue and obtain privacy. (Cal. Const., art. I, § 1.)

2) Establishes the Insurance Information and Privacy Protection Act (IIPPA), to establish standards for the collection, use, and disclosure of information gathered in connection with insurance transactions and to maintain a balance between the need for information by those conducting the business of insurance and the public's need for fairness in insurance information practices. (Ins. Code § 791.)

3) Requires an insurance institution or agent to provide a notice of information practices to all applicants or policyholders in connection with insurance transactions at the time of delivery or initial data collection and at the point of renewal, reinstatement, and change in benefits, as provided. (Ins. Code § 791.04.)

4) Authorizes an insurer to disclose personal or privileged information about an individual, which is collected or received in connection with an insurance transaction, as provided. This includes the authority to share personal or privileged information about an individual with an unaffiliated third party whose only use of the information will be in connection with the marketing of a product or service, as long as the individual is given an opportunity to opt out of this information-sharing. (Ins. Code § 791.13.)

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

6) 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. (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.)

7) Establishes the California Privacy Protection Agency (Privacy Agency), vested with full administrative power, authority, and jurisdiction to implement and enforce the CCPA. The Privacy Agency is governed by a five-member board, with the chairperson and one member appointed by the Governor, and the three remaining members are appointed by the Attorney General, the Senate Rules Committee, and the Speaker of the Assembly. (Civ. Code § 1798.199.10.)

8) Directs the Privacy Agency 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 this title. Upon completing its review, the agency 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. (Civ. Code § 1798.185(a)(20).)

9) Establishes the Data Broker Registration Law (DBRL). (Civ. Code §§ 1798.99.80-1798.99.88.)

10) Defines a "data broker" as a business that knowingly collects and sells the personal information of a consumer to a third party that the business does not have a direct relationship with. (Civ. Code § 1798.99.80.)

11) Requires data brokers to register annually with the Privacy Agency and provide specified information. (Civ. Code § 1798.99.82.)

12) Requires the Privacy Agency, by January 1, 2026, to develop an accessible deletion mechanism that allows a consumer to request that every registered data broker delete any personal information held by the broker. (Civ. Code § 1798.99.86.)

13) Permits amendment of the CPRA 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 § 25 (2020).)

THIS BILL:

1) Establishes standards for the collection, processing, retaining, or sharing (collectively referred to as "processing") of a consumer's personal information by licensees, surplus line insurers, reinsurers and their third-party service providers.

2) Requires the standards to address all of the following:

   a) Protect consumers' personal information processed by licensees, surplus line insurers, reinsurers, or their third-party service providers.

   b) Inform consumers of the categories of personal information being processed.

c) Inform consumers of the categories of sources from which consumers' personal information is collected and identify recipients when the information is shared.

d) Permit consumers to choose whether to opt in to the sharing of their personal information for purposes other than insurance transactions.

e) Permit individual consumers to request access to their personal information to verify or dispute the accuracy of the information.

f) Inform consumers of the reasons for adverse underwriting decisions.

g) Require data minimization practices for all licensees, surplus line insurers, reinsurers, and their third-party service providers in the processing of consumers' personal information.

h) Provide accountability for the improper processing of consumers' personal information by licensees, surplus line insurers, reinsurers, and their third-party service providers in violation of the bill.

2) Provides consumers with the following rights and protections:

a) The right to correct, amend, or delete any personal or publicly available information about the consumer.

b) The right to request any personal and publicly available information that is in possession of the licensee, surplus line insurer, reinsurer, or third party service provider (TPSP).

c) Prohibits a licensee, surplus line insurer, reinsurer, or TPSP from processing a consumer's personal information for a purpose that the consumer did not consent to.

d) States that consent is not established by any of the following means:

i) Acceptance of a general or broad terms of use or similar document that contains descriptions of personal information processing, along with other unrelated information.

ii) Hovering over, muting, pausing, or closing a given piece of content.

iii) Agreement obtained through the use of dark patterns.

e) Requires the licensee, surplus line insurer, reinsurer, or TPSP obtain prior, opt-in consent from the consumer before sharing their personal information for the marketing of a product or service, or for a research activity.

f) Requires the licensee, surplus line insurer, reinsurer, or TPSP to offer an opt-out option to consumers before sharing their personal information for certain purposes, including:

i) The joint marketing of cobranded financial products or services.

(1) Limits the personal information to name; address or email address; financial institution affiliation and account type; and age.

ii) The cross-marketing of insurance or financial products or services.

iii) In connection with FAIR Plan clearinghouse activities.

g) Strictly prohibits the sale of consumers' personal information.

3) Requires a licensee, surplus line insurer, reinsurer, or TPSP to provide the notices required pursuant to the bill.

4) 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.

5) 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.

6) 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.

7) 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.

8) Makes several procedural clarifications 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.

9) 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.

10) 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:

a) In connection with an insurance transaction, as defined, or provision of "value added services or benefits" in connection with an insurance transaction, as defined.

b) For compliance with legal requirements.

c) 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.

d) 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.

e) 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.

f) 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.

11) 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:

a) 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.

b) 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.

c) 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.

15) 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:

a) In connection with the joint marketing of cobranded financial products or services between a licensee and a financial institution, as specified.

b) 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.

c) 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.

d) In connection with FAIR Plan clearinghouse activities, as specified.

e) For additional purposes specified by the commissioner in regulation.

16) Prohibits a licensee, surplus line insurer, reinsurer, or TPSP from processing a consumer's sensitive personal information, other than in connection with an insurance transaction.

17) 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.

18) 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.

19) 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.

20) 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.

21) 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.

22) 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.

23) 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.

24) Requires a licensee, surplus line insurer, reinsurer, or TPSP to promptly provide notice to the commissioner of an incident constituting a breach, as specified.

25) 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.

26) Requires a licensee, surplus line insurer, reinsurer, or TPSP that, pursuant to an insurance transaction, takes title to a vehicle storing personal information of a consumer, shall restore the vehicle to its factory default setting thereby removing a consumer's personal information before selling or transferring the vehicle.

27) States that the requirements related to a vehicle are satisfied if any of the following apply:

    a) The licensee, surplus line insurer, reinsurer, or TPSP determines that the damage to the vehicle's electrical system prevents any access to the components storing personal information.

    b) The licensee, surplus line insurer, reinsurer, or TPSP makes all reasonable attempts to power on the vehicle and the vehicle is not able to be powered on.

    c) The vehicle is determined to contain a biohazard or other hazardous conditions that would make access unsafe.

    d) Accessing the components could create a reasonable risk to the health and safety of an employee.

    e) The licensee, surplus line insurer, reinsurer, or TPSP destroys or renders unreadable the personal information stored on the vehicle.

28) Prohibits retaliation against a consumer for the exercise of rights pursuant to the IIPPA.

29) Increases penalties for knowing and willful violations of the provisions of the IIPPA.

30) Provides several rights and authorities to the commissioner to enforce, and clarify through regulations and rulemaking, the provisions of the bill.

31) 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.

32) Makes conforming and technical changes to existing provisions of the IIPPA.

33) Defines various terms, among them:

    a) "Aggregated consumer information" means information that relates to a group or category of consumers, that is deidentified, and that is not linked or reasonably linkable to a consumer, household, or specific electronic device.

    b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics that can be used, singly or in combination with other identifying information, to establish a consumer's identity. Biometric information may include an iris or retina scan, fingerprint, face, hand, palm, ear, or vein pattern, or voiceprint, from

which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, or any other means to identify an individual.

c) "Clear and conspicuous notice" means a notice that is reasonably understandable and designed to call attention to the nature and significance of its contents.

d) "Collect" or "collecting" means buying, renting, licensing, gathering, obtaining, receiving, or accessing a consumer's personal information.

e) "Consent" means a freely given, specific, informed, and unambiguous indication of the consumer's wishes by which the consumer, or the consumer's legal guardian, a person who has power of attorney, or a person acting as a conservator for the consumer, including by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the consumer for a narrowly defined particular purpose.

f) "Consumer" means an individual who is a resident of California whose personal information is processed or has been processed in the business of insurance, including a current or former applicant, claimant, beneficiary, policyholder, insured, participant, annuitant, employee, or certificate holder. "Consumer" includes an individual's legal representative.

   i) A consumer is in an ongoing business relationship with a licensee, surplus line insurer, or reinsurer if there is a continuing relationship between the consumer and the licensee, surplus line insurer, or reinsurer based on one or more insurance transactions provided by the licensee, surplus line insurer, or reinsurer.

   ii) A consumer is a resident of this state if the consumer's last known mailing address, as shown in the records of the licensee, surplus line insurer, or reinsurer, is in this state unless the last known address of record is deemed invalid.

   iii) "Consumer" does not include an individual in the course of the individual acting as a job applicant to, or an employee, director, officer, or independent contractor of, a licensee, surplus line insurer, reinsurer, or third-party service provider, to the extent that the individual's personal information is processed by the licensee, surplus line insurer, reinsurer, or third-party service provider solely within the context of the individual's role or former role as a job applicant to, or an employee, director, officer, or an independent contractor of, that licensee, surplus line insurer, reinsurer, or third-party service provider.

g) "Cross marketing" means marketing of insurance or financial products or services by or on behalf of a licensee, to a consumer with which the licensee has an ongoing business relationship. Cross marketing includes an insurance or financial product or service, whether offered by the licensee or by a third party.

h) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decisionmaking, or choice.

i) "Deidentified information" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a licensee, surplus line insurer, or reinsurer that processes deidentified information meets all the following criteria:

   i) (A) Has implemented reasonable technical safeguards and policies designed to prohibit reidentification of the consumer to whom the information may pertain.

   ii) Has implemented reasonable business policies that specifically prohibit reidentification of the information.

   iii) Has implemented business processes designed to prevent inadvertent release of deidentified information.

   iv) Makes no attempt to reidentify the information.

   v) Does not retain any sensitive personal information.

   vi) Other requirements pertaining to deidentification that the commissioner specifies in regulation.

   vii) Deidentified information is not personal information.

j) "Insurer" means any of the following:

   i) A corporation, association, or partnership required to be licensed by the commissioner to assume risk or otherwise authorized to assume risk, including a reciprocal exchange, interinsurer, fraternal benefit society, or multiple-employer welfare arrangement.

   ii) A self-funded plan subject to regulation by the commissioner.

   iii) A preferred provider organization administrator.

   iv) The servicing of an insurance application, policy, contract, or certificate. "Insurer" does not include producers, insurance support organizations, foreign-domiciled risk retention groups, reinsurers, or surplus line insurers.

k) "Personal information" means information processed in the business of insurance 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.

l) "Personal information" includes any of the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

   i) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

ii) Personal information described in subdivision (e) of Section 1798.80 of the Civil Code.

iii) Characteristics of protected classifications pursuant to state or federal law.

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

v) Biometric information.

vi) Internet or other electronic network activity information, including browsing history, search history, and information regarding a consumer's interaction with an internet website, online platform, digital application, or advertisement.

vii) Geolocation data.

viii) Auditory, electronic, visual, thermal, olfactory, or other sensory information.

ix) Professional or employment-related information.

x) Education information that is not publicly available, personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g) and related regulations (Part 99 (commencing with Section 99.1) of Title 34 of the Code of Federal Regulations).

xi) Sensitive personal information.

m) "Personal information" means any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. "Personal information" includes an individual's name and address and "medical record information" but does not include "privileged information," psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

n) "Personal information" does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern.

o) "Process," "processing," or a "process" means 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.

p) "Publicly available" means information about a consumer that a licensee, surplus line insurer, reinsurer, insurance support organization, or third-party service provider has a reasonable basis to believe is lawfully made available from any of the following:

i) Federal, state, or local government records.

ii) Widely distributed media.

iii) Disclosures to the general public that are required to be made pursuant to federal, state, or local law.

q) "Publicly available" does not mean biometric information collected about a consumer without the consumer's knowledge.

r) "Reinsurer" means a legal entity primarily engaged in assuming all or part of the risk associated with existing insurance policies originally underwritten by insurers, or a legal entity known as a "retrocessionaire" that accepts all or part of one or more reinsurance policies issued by a reinsurer.

s) "Research activities" means systemic investigation, including development, testing, and evaluation, designed to develop or contribute to generalizable knowledge if there is sharing of personal information with nonaffiliated third parties.

t) "Retain," "retention," or "retaining" means storing or archiving personal information that is in the continuous possession, use, or control of a licensee, surplus line insurer, reinsurer, or third-party service provider.

u) "Sale," "sell," or "selling" means the exchange of personal information to a third party for monetary or other valuable consideration. "Sale" of personal information does not include any of the following sharing of personal information:

i) Disclosing information to a third-party service provider for the purpose of or in support of providing an insurance or financial product or service requested by the consumer.

ii) Sharing with or receiving information from an insurance support organization, statistical agent, or reinsurer in connection with an insurance transaction.

iii) Providing or disclosing information to an affiliate or in connection with joint marketing activity as permitted by this article.

iv) Transferring personal information to a third party as an asset pursuant to a merger, acquisition, bankruptcy, or other transaction, or a proposed merger, acquisition, bankruptcy, or other transaction in which the party assumes control of all or part of the licensee's, surplus line insurer's, or reinsurer's assets.

v) Disclosure pursuant to a consumer's direction to the licensee, surplus line insurer, reinsurer, or third-party service provider to disclose personal information to, or interact with, one or more third parties.

v) "Sensitive personal information" means personal information that reveals any of the following information about a consumer:

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

ii) Account login, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

iii) Precise geolocation.

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

v) Content of personal mail, personal email, personal text messages, or personal voice or video communications, unless the person in possession is the intended recipient of the communication.

vi) Genetic or neural data.

vii) Information about the consumer's sex life or sexual orientation.

viii) Health information.

ix) Biometric information.

x) Additional items specified by the commissioner in regulation.

w) Sensitive personal information that is publicly available shall not be considered sensitive personal information or personal information.

x) "Share," "shared," or "sharing" means sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by a licensee, surplus line insurer, reinsurer, or third-party service provider to a third party.

y) "Third-party service provider" means a person, including directors, officers, employees, and agents thereof, that contracts with a licensee, surplus line insurer, or reinsurer to provide services to the licensee, surplus line insurer, or reinsurer, to the extent that it processes, shares, or otherwise is permitted access to personal information through its provision of services to the licensee, surplus line insurer, or reinsurer. "Third-party service provider" includes insurance support organizations and a person with whom a licensee, surplus line insurer, or reinsurer does not have a continuing business relationship and does not have a contract, but may have to share personal or publicly available information in connection with an insurance transaction pursuant to subdivision (c) of Section 791.24.

z) "Third-party service provider" does not include governmental entities, licensees, affiliates of licensees, surplus line insurers, reinsurers, or data brokers registered pursuant to Section 1798.99.82 of the Civil Code.

COMMENTS:

1) **Author's statement**. 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. Modern-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 with.

2) **Historical perspective.** To fully understand how completely people in California and throughout the country have ceded the right to live their lives in private, free from both government and private surveillance, privacy experts reflect on the concerns raised by federal and state lawmakers 50 years ago when debating the creation of the FBI's National Crime Information Center's computerized data collection system (NCIC). This database that was so controversial at the time simply allowed local, state, and federal law enforcement agencies to share personal data related to suspected criminal activities. Congress held "days and days" of hearings over two years. Members warned of the "threat of the dictatorship of dossiers."[1]

During the debates, Senator Barry Goldwater of Arizona lamented, "Where will it end? . . . Will we permit all computerized systems to interlink nationwide so that every detail of our personal lives can be assembled instantly for use by a single bureaucrat or institution?"[2] Senator Charles H. Percy of Illinois in foreshadowing of what would come to pass in the 21st century warned:

> I hope that we never see the day when a bureaucrat in Washington or Chicago or Los Angeles can use his organization's computer facilities to assemble a complete dossier of all known information about an individual. But, I fear that is the trend. . . . Federal agencies have become omnivorous fact collectors—gathering, combining, using, and trading information about persons without regard for his or her rights of privacy. Simultaneously, numerous private institutions have also amassed huge files . . . of unprotected information on millions of Americans.[3]

During the same period when Congress was expressing concern about the erosion of individuals' privacy protections, the people of California used the initiative process to add "privacy" to the list of "inalienable rights" in the state constitution in 1972.[4] Proponents noted the initiative was specifically designed to preserve Californians' private lives and fundamental rights in the face of technological advances. They argued: "The right of privacy is the right to be left alone. . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes. . . ."[5]

---

[1] Citron, Danielle Keats, *A More Perfect Privacy,* 104 Boston University Law Review, 1073–1086 (2024).
[2] *Ibid.*
[3] *Ibid.*
[4] California Proposition 11 (1972), "Constitutional Right to Privacy Amendment."
[5] *Right of Privacy California Proposition 11*, UC L. SF SCHOLARSHIP REPOSITORY (1972), pp. 26–27, https://repository.uclawsf.edu/cgi/viewcontent.cgi?article=1761&context=ca_ballot_props.

Presently, California voters face an even greater "dictatorship of dossiers"[6] than their predecessors, with not only global governments' ability to monitor individuals' private lives, but also the near ubiquitous access to these dossiers afforded to private businesses and individuals willing to pay for them. There are more than 4,000 data brokers with dossiers on 98% of the people in the United States.[7] The largest data broker, Acxiom, has more than 10,000 data attributes on over 2.5 billion people in more than 60 countries.[8] The amount of data being collected on people has increased dramatically over the last decade as businesses have figured out how to monetize this natural resource.[9]

3) **California's Consumer Privacy Laws.** 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; 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 an 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, except under certain circumstances.

In 2018, the Legislature enacted the CCPA (AB 375; Chau, Chap. 55, Stats. 2018), which gave consumers certain rights regarding their personal information,[10] such as the right to: (1) know what personal categories of information about them are collected and sold; (2) request the deletion of personal information; and (3) opt-out of the sale of their personal information, or opt-in, in the case of minors under 16 years of age. The CCPA was the first general data privacy law of its kind in the nation.

In 2020, California voters passed Proposition 24, the California Privacy Rights Act (CPRA), which both established additional privacy rights for Californians and arguably weakened other privacy rights. Chief among these additional rights was the right of a consumer to limit a business's use of sensitive personal information.[11] Importantly, as it pertains to the interaction between the IIPPA reforms included in this bill and the CCPA, one of the most important components of Proposition 24 was establishing that the CCPA, as amended, was a floor and not a ceiling for privacy protection. Essentially, to protect Californians from any future legislative efforts to weaken statutory protections in the CPRA, Proposition 24 provided that the CPRA's contents may be amended by a majority vote of the Legislature if the amendments are consistent

---

[6] Clarke, Laurie. "Interview - Law professor Danielle Citron: 'Privacy is essential to human flourishing,'" *The Guardian* (Oct. 2, 2022) https://www.theguardian.com/technology/2022/oct/02/danielle-citron-privacy-is-essential-to-human-flourishing.
[7] Solove, Daniel J. *Privacy in Authoritarian Times: Surveillance Capitalism and Government Surveillance*, George Washington University Law School (Jan. 19, 2025). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5103271.
[8] *Ibid.*
[9] *Ibid.*
[10] Civ. Code § 1798.140(v).
[11] Civ. Code § 1798.140(ae).

with and further the purpose and intent of the CPRA, which is to further protect consumers' rights, including the constitutional right of privacy.

Among the provisions, section 1798.185 of the Civil Code, enacted by Proposition 24, tasks the Attorney General, and later the newly created Privacy Agency with promulgating regulations for several specified reasons critical to the implementation of the CCPA. As it relates to the IIPPA, 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 [Privacy Agency] 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 the Privacy Agency 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 Privacy Agency maintains jurisdiction over other aspects of data privacy in the insurance industry to the extent provisions of CCPA are stronger than their counterparts in the Insurance Code. As a result, regulatory and enforcement authority are split between the Privacy Agency and the Insurance Commissioner, and compliance is exceedingly complex.

4) **The need for this bill.** The IIPPA was enacted in 1980, well before the internet and computer technology transformed how data is collected, stored, and shared. The law does not adequately address modern challenges like algorithmic decision-making, big data analytics, cloud storage, or online data collection methods used by relevant parties. Furthermore, the act's consent mechanisms and disclosure requirements were not designed for digital interfaces in today's data-driven insurance industry.

This bill seeks to establish an updated privacy framework for insurance consumers to reflect advances in technology and to ensure that the IIPPA is more privacy protective than the CCPA in order to make it clear that the Insurance Commissioner has sole responsibility for regulating insurance.

The author explains the need for the bill in this way:

> The Insurance Information and Privacy Protection Act (IIPPA), provides protections for personally identifiable information, generally provided to insurance professionals like agents, brokers or insurance companies in order to apply for insurance or submit a claim. Many of the provisions were enacted in the 1980's and do not address all of the advancements in technology and the ways consumer data can be used.
>
> More than almost any industry, insurance companies require significant amounts of personal information from consumers in order to properly manage risks. Increasingly, licensees are using sophisticated technologies to collect and process consumers' personal information,

> which has increased the volume and sensitivity of personal information that licensees collect about consumers. Developments in insurance business structures have led to increasingly complex contracting arrangements between licensees and service providers, with the attendant risk in supply chain data breaches. There is a lack of oversight into how much data licensees collect, what purposes it can be used for, who it can be shared with, and how long it can be retained.
>
> Additionally, the California Consumer Privacy Act (CCPA) was later expanded by the California voters with the passage of Proposition 24. These existing privacy laws mandate the Consumer Privacy Protection Agency to adopt regulations applying privacy protections to insurance licensees if California's Insurance Code and regulations do not provide stronger privacy protections. This bill is intended to provide stronger protections that support the intent of CCPA.

The Insurance Commissioner, sponsor of the bill, further explains:

> Existing California insurance privacy laws are more than 40 years old and consumer privacy protections have been outpaced by modern insurance industry business practices, exposing consumers to considerable risk. The original drafters of these legacy laws could not have anticipated the fluidity with which PI is currently collected, the many new purposes for which PI is processed and exchanged, or the scale and speed at which these transactions take place.
>
> Institutionalized hacking is a reality and data-rich entities like insurance businesses are targeted by bad actors. Between 2017 – 2021, California led the nation in data breaches, with 325,291 victims losing more than $3.7 billion. In 2025, the global average cost of a data breach reached $4.88 million per Incident.

5) **What this bill would do.** This bill seeks to more clearly establish the general jurisdiction of the Insurance Commissioner over data privacy rights of insurance consumers. Specifically, 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. Toward that end:

- Strengthens consumer rights by doing the following –
    - Providing the right for consumers to opt in to the sharing of personal information by licensees for purposes unrelated to insurance transactions; provides limited opt-out for specified marketing purposes.
    - Providing the right to review, correct, and delete personal and publicly available data that licensees have about consumers.
    - Providing the right for consumers to access the personal information that is processed, the sources from where the information is collected, and to identify recipients when information is shared, as well as disclosing the reasons for adverse underwriting decisions.

- Providing opt-in and opt-out rights for the use of personal information for marketing purposes.
- Providing the right to exercise these rights without retaliation from their insurer.
- Providing the right to delete inaccurate or unnecessary personal information.
- Prohibiting the sale of consumers' personal information for any consideration.

- Increases obligations for insurance licensees –

  - Requires that contractual arrangements between insurers and vendors protect personal consumer data and that the information is only used for the reason it was requested.
  - Requires insurance companies to develop policies and procedures related to records retention and deletion, including securely destroying personal information that is no longer needed.
  - Requires licensees to establish and follow protocols to protect consumers' personal information and provide data breach notifications to the California Department of Insurance.
  - Requires licensees properly vet and oversee service providers they engage, including requiring the third-party provider to ensure that those accessing the personal information are subject to a duty of confidentiality, to maintain appropriate safeguards to ensure protection of any personal information, and to not further process or disclose the personal information obtained from, or on behalf of, the licensee other than as specifically stated in the contract.
  - Limits when and how a licensee can process a consumer's personal information.
  - Requires that collection, processing, retention, or sharing of the consumer's personal information comply with the most recent privacy notice provided.
  - Requires the processing and retention of the information must be reasonably necessary and proportionate to achieve the purposes related to an insurance transaction or other purpose the consumer requested or authorized and not further processed in a manner that is incompatible with those purposes.
  - Prohibits licensees from processing sensitive personal information other than in relation to an insurance transaction.

6) **Significant distinctions between the IIPPA and the 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. As discussed in the detailed Insurance Committee analysis, 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."[12]

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 right for a 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, which, in the context of this bill, are primarily independent agents and brokers.

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

[12] The June 26, 2026 amendments making several new distinctions between "processing" and "sharing," particularly when it comes to opting in or out of the sharing of personal information.

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.

ARGUMENTS IN SUPPORT: California Insurance Commissioner Ricardo Lara, the sponsor, writes in support of a previous version of this bill:

> SB 354 will enhance the Insurance Information and Privacy Protection Act. This landmark legislation recognizes that California consumers have the right to reasonable privacy protections that address the demands of an information-intensive insurance business climate. Under this bill, insurers would be required to follow clear standards for collecting and using personal data, ensuring that information is gathered for the purpose required by the consumer, unless otherwise specified. SB 354 would prohibit the sale of consumers' personal information for any reason, and guarantee consumers the rights to access, verify, correct, or dispute the accuracy of information held about them. To reinforce these protections, this bill would mandate robust data minimization and retention limits to ensure only information necessary for underwriting, servicing, or claims handling is collected and retained, and establishes accountability and enforcement mechanisms to prevent improper processing or misuse of consumer data by insurers and their services providers.
>
> 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 privacy 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 continue to demonstrate how consumers' sensitive personal information is a prime target, especially among data-rich industries such as insurance.
>
> Voters passed Proposition 24, the California Privacy Rights Act (CPRA) of 2020, which expanded consumer privacy rights and expressly extended the application of CPRA's requirements to insurance licensees when California's insurance statutes and regulations do not provide stronger privacy protections than what are found in the CPRA. SB 354 upholds our state's constitutional values by furthering the purposes and intent of CPRA to ensure California's insurance laws enable my Department – as the state's insurance regulatory entity – with the necessary authority to adequately and fairly regulate the insurance industry.
> I remain committed to creating long-term policy solutions for consumers so that we can build a stable and sustainable insurance market that works for all Californians. In order to do that, we need to ensure that California's insurance privacy laws are both responsive to protecting consumers and reflect modern business practices in the insurance market.

I remain committed to creating long-term policy solutions for consumers so that we can build a stable and sustainable insurance market that works for all Californians. In order to do that, we need to ensure that California's insurance privacy laws are both responsive to protecting consumers and reflect modern business practices in the insurance market.

Arguing in support of a previous version of this bill, Oakland Privacy notes:

Technology has significantly revolutionized many aspects of people's lives and businesses across most industries. Insurance is no exception. California's insurance privacy regulations were last updated several decades ago, leaving large gaps given the innovations in the insurance industry. The industry has embraced the benefits of technology – in particular the ability to collect vast amounts of data. Insurance companies heavily use artificial intelligence processing and data analytics, chatbots for customer communications, connected devices and telematics, and drones for inspection.

As an example, the "newfangled" insurance company Lemonade is said to collect 1,500 data points on each customer. State Farm has filed many patents to manage risk and aid in pricing. This has become very lucrative for insurance – in 2024, over 13,000 patents were filed for insurance data analytics. In the previous year (2023) there were just under 2,000 patents. According to research, the insurtech market is estimated to surpass $52 billion in 2025.

The insurance industry is benefiting from the troves of data they are collecting including reducing their risk exposure – but those benefits aren't necessarily translating to an improved consumer experience. State Farm dropped the insurance policies of 72,000 Californians in 2024. Instead, customers are increasingly seeing their privacy being put at risk. Particularly disturbing is the push to collect continuous streams or "real-time data" to adjust a consumer's premiums based on dynamic changes in their behavior.

One of these pervasive practices is telematics when vehicles collect troves of data such as locational coordinates which track a vehicle's whereabouts, navigation destinations from GPS networks, and remote control information. A recent report researching 25 car brands found that vehicles were the worst privacy offenders of various technological devices across various industries and product categories that had been reviewed. Vehicles were found to collect vast amounts of information on drivers (and passengers) including sexual activity, immigration status, race, facial expressions, weight, health and genetic information to facilitate the automobile insurance industry, The report shows that car manufacturers and their vendors collect far too much personal data despite their "Consumer Protection Principles" which included assurances that they protect people's private information.

Moreover, most manufacturers did not provide consumers meaningful control over their data. Chevy collected information relating to driving habits, and shared that data with insurance providers, leading to increased rates or policy cancellations. GM has also been found to share data with LexisNexis Risk Solutions with negative impacts on consumer's insurance policies.

It is apparent that consumers are being encouraged, incentivized and in some cases required, to give up excessive amounts of data. The insurance industry has reasonable needs for customer information to assess risk, but in return customers can and should demand that information be properly used, secure, and not weaponized against them.

[. . .]

Because insurance-related information is often intrinsically sensitive, we wanted to highlight a few of the protections in Senate Bill 354 that need to remain robust to protect consumers:

1. Third party contractor requirements in section 791.24 which are explicit about written agreements with contractors and place accountability with insurance companies for the behavior of their third party contractors.

2. Clear data retention and deletion standards and justifications in section 791.30

3. An explicit ban on "dark pattern" obscured consent mechanisms in section 791.31

4. Robust rights of correction, amendment and deletion in section 791.09

5. Investigation and enforcement functions as defined in sections 791.14 to section 791.19

6. We know that the companies want broad permissions, including an opt-out rather than an opt-in, for marketing purposes and to share information within their "families of companies". We want to emphasize that many insurance companies are company-family with data broker companies and that there needs to be a very robust consent process for these kinds of marketing relationships. As a result of the data broker industry, we have data that demonstrates that family members of insurers are data brokers that are selling children's data, repro data, and location info, In our opinion, it should be opt-in, but if it must be opt-out it needs to be clear, conspicuous and stand-alone.

7. The CA Department of Insurance should track and publish known data breaches in the insurance field, as the Cal Privacy currently does for the business sectors they oversee.

ARGUMENTS IN OPPOSITION: In opposition to a previous version of the bill, a coalition of insurance associations argues:

We have had continued fruitful negotiations with the Pro Tem's office and the Department of Insurance. While we have not yet fully solidified the necessary amendments to address the serious operational issues in the bill there have been indications from the author and the sponsor that they intend to address them.

Our industry has always supported robust, insurance specific regulations to protect our customers, and we remain actively engaged with regulators, including CDI, through the National Association of Insurance Commissioners (NAIC) effort to craft an updated privacy model. The NAIC Privacy Protections (H) Working Group's work to update Model 672 is expected to be completed in 2027 and would not only modernize the provisions that SB 354 aims to address,

but would allow for an adoptable, more uniform Model. This uniformity helps consumers, regulators, and insurers and allows for more cost-efficient compliance.

While the goal of SB 354 has been to set the heightened privacy standard, it has established standards that are fundamentally unachievable, create confusion about who is subject to the Act, and compromise the ability of insurers and agents to offer insurance to consumers desperate for a functional market.

The joint trades listed above are committed to finding a functional solution to the bill and have provided amendments to the author and the CDI, which would establish the highest insurance consumer privacy protection standards in the nation and exceed CCPA, without crippling the business of insurance.

It is absolutely critical that SB 354 adopt our proposed language to do the following:

1.Definitions: Specifically, address issues within "insurance transaction" and "research activity" to ensure that backend processing and product development are not so hindered that California consumers are left with products decades behind consumers in other states.

2.Notices: Address scope issues which would result in notices going to beneficiaries and named insureds rather than to the policyholder, as well as clarify that the disclosures remain meaningful by changing the disclosed purposes to "categories" of purposes. The change regarding disclosures was also addressed throughout other provisions of the bill for conformity.

3.Data Minimization and Sharing: This section of the bill remains the most problematic. By treating "processing" as one and the same with "sharing" it creates hurdles to the processing of consumer data for functionality of the policy. The heightened opt-in standard for certain forms of processing would exceed even the EU's Global Data Protection Regulation. There has been no justification for why insurers, whom consumers actively seek out, should be the test subjects for the world's most stringent data-processing rule. Particularly at a time when market stabilization has been a primary priority.

4.Private Right of Action: 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. We have requested that the PRA provision be returned to the existing scope of rights protected under the Act.

It is our hope that these operational issues will be addressed in forthcoming amendments. However, as of this writing, they remain at issue. As you are well aware, many lines of insurance are struggling within the current economic climate, and the property casualty insurance industry in particular is currently in crisis and needs to focus its efforts on effectively serving Californians and maintaining a stable and diverse insurance marketplace within the state.

In addition, a coalition of independent agents, led by the Independent Insurance Agents & Brokers of California, writes in opposition to a previous version of the bill:

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.

The CCPA recognized that this result is impractical and unnecessary for small businesses that do not engage in the same data practices as the entities the law principally targeted. It therefore included a small-business exemption. SB 354 should take a similar approach. Without that change, the bill would impose costly and expansive compliance obligations on independent producers that are disproportionate to their role in the insurance delivery system and beyond the capacity of many small business members to implement.

For example, in an abbreviated form, SB 354 would require all “Licensees” to implement measures such as the following:

- Provide detailed privacy notices at the start of each consumer relationship, including categories of data collected, sources, purposes, sharing practices, and consumer rights, in prescribed formats and accessible languages.

- Obtain affirmative consumer consent before using personal information outside the core insurance transaction and maintain written records of each consent and revocation.

- Establish written procedures for selecting and overseeing third-party vendors and incorporate extensive data protection requirements into vendor contracts.

- Create systems to acknowledge and respond to consumer access requests, notify third parties when required, and maintain a toll-free response channel.

- Provide written explanations for adverse underwriting decisions, including specific reasons and data elements involved, even though producers do not make those decisions.

- Adopt written records-retention schedules and conduct annual reviews of consumer records to determine whether data must still be retained.

- Implement and maintain administrative, technical, and physical information security programs, including prompt breach reporting to the Insurance Commissioner.

- Retain compliance records for the current year and preserve consumer consent records throughout the duration of the relationship.

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. Those compliance structures are designed for large institutions, not individual producers and small agencies operating without a size-based exemption.

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.

REGISTERED SUPPORT / OPPOSITION:

Support

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

Opposition

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
California Agents and Health Insurance Professionals
California Chamber of Commerce
California Credit Union League
California Insurance Wholesalers Association
Civil Justice Association of California (CJAC)
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
National Insurance Crime Bureau
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 and Information Industry Association
Software Information Industry Association
Techca

TechNet
The Committee of Annuity Insurers

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