Date of Hearing: April 23, 2019

ASSEMBLY COMMITTEE ON PRIVACY AND CONSUMER PROTECTION
Ed Chau, Chair
AB 981 (Daly) – As Amended April 12, 2019

SUBJECT: Insurance Information and Privacy Protection Act

SUMMARY: This bill would exempt insurance institutions, agents, and support organizations (insurers) to which the Insurance Information and Privacy Protection Act (IIPPA) applies from the California Consumer Privacy Act of 2018 (CCPA), except as specified. The bill would also, among other things, incorporate specific concepts from the CCPA into the IIPPA. Specifically, **this bill would**:

1) Provide that insurers or insurance transactions subject to the IIPPA shall be exempt from the CCPA. This exemption does not apply to the limited private right of action for data breaches in the CCPA or business activity not subject to the IIPPA.

2) Define various terms for the purposes of the IIPPA including, among others: "aggregate consumer information," "biometric information," and "deidentified" to mirror the definitions provided in the CCPA; "consumer" to reflect the definition proposed in the March 25, 2019 version of AB 25; "PI" to reflect the definition of that term provided in the CCPA, with the exception of "household," which is absent from the definition, similar to AB 873 (Irwin).

3) Require insurers to provide a notice of information practices, including the categories of PI that may be collected and the purposes for which the categories of PI may be used, to all applicants or policyholders in connection with insurance transactions and to the general public.

4) Require an insurers to provide a clear and conspicuous notice that accurately reflects its privacy policies and practices as follows:

    - To an applicant or policyholder, not later than at the time the insurer establishes a customer relationship, except as provided below in #5.

    - To an applicant or policyholder before the insurance institution or agent discloses any nonpublic PI about the applicant or policyholder to any nonaffiliated third party, as specified.

5) Authorize an insurer to provide the initial notice required within a reasonable time after the insurer establishes a customer relationship under any of the following circumstances:

    - If establishing the customer relationship is not at the policyholder's election, as specified.

    - If providing notice at the time the insurer establishes a customer relationship would substantially delay the individual's transaction, including if the insurer and the individual agree by telephone to enter into a customer relationship involving prompt delivery of the insurance product or service. In that case, the individual must be provided with oral notice of the insurer's privacy policies, provided that the privacy notice is mailed or sent in electronic form within 14 business days after the sale, as specified.

- If the relationship is initiated in person at the insurance institution's or agent's office or through other means and the individual may view the notice on an internet website or other source.

6) Authorize an insurer to notify a policyholder about their right to delete, if appropriate, PI in an abbreviated notice.

7) Include on a disclosure required before insurers can share PI the following, among other things:

   - The text "IMPORTANT PRIVACY CHOICES" in 16-point boldface type.

   - Reasonable means by which the individual may exercise the right to opt out of any disclosure at any time.

   - That an individual's direction to opt out of the disclosure is effective until the individual revokes that direction in writing or electronically, at the individual's choice.

8) Require, after any individual submits a written request for access to recorded PI about themselves, as specified, that the insurer shall, among other things, do the following within 30 days:

   - Inform the individual of the *categories* and *sources* of recorded PI, as specified.

   - Inform the individual of the business or commercial purpose for collecting or selling PI.

   - Permit the individual to obtain a copy of such the recorded PI in a safe and secure electronic manner or by mail, whichever the individual prefers, unless the recorded PI is in coded form, in which case an accurate translation in plain language shall be provided in writing.

9) Add "or other verifiable request" to the IIPPA provision providing individuals with the process by which to amend, delete, or dispute recorded PI.

10) Authorize an insurer to disclose PI without the individual's consent for research studies, as specified.

11) Require an insurance institution, agent, or insurance-support organization to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of policyholder information, as specified, and authorize the commissioner to audit an insurance intuition, agent, or support organization's compliance with this requirement. The insurer shall do all of the following:

   - Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of policyholder information or policyholder information systems.

   - Assess the likelihood and potential damage of the internal and external threats, taking into consideration the sensitivity of policyholder information.

- Assess the sufficiency of policies, procedures, policyholder information systems, and other safeguards in place to control risks.

- Train staff, as appropriate, to implement the information security program.

- Regularly test or otherwise regularly monitor the key controls, systems, and procedures of the information security program. The frequency and nature of the tests shall be determined by the insurer's risk assessment.

- Exercise appropriate due diligence in selecting service providers, and require them to implement appropriate measures designed to meet the objectives of this section.

- Monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its policyholder information, internal or external threats to information, and the insurance institution's, agent's, or insurance-support organization's own changing business arrangements, including mergers and acquisitions, outsourcing arrangements, and changes to policyholder information systems.

12) Grant a policyholder the right to request and receive a copy of the policyholder's PI from an insurer in a readily usable format that can be transferred to another entity.

13) Prohibit an insurer from selling the PI of an insured if the insurer has actual knowledge that the insured is less than 16 years of age, unless the insured, in the case of an insured between 13 and 16 years of age, or the insured's parent or guardian, in the case of an insured who is less than 13 years of age, has affirmatively authorized the sale of the insured's PI. An insurer that willfully disregards an insured's age shall be deemed to have had actual knowledge of the insured's age. This right may be referred to as the "right to opt in." (This is based on the right of minors (age 13 to 16, as specified), to opt-in to the sale of their PI in the CCPA.)

14) Prohibit an insurer from "unfairly discriminating," as defined, against an applicant or policyholder because that applicant or policyholder has:

    - Opted out from the disclosure of nonpublic PI.

    - Not granted authorization for the disclosure of nonpublic personal medical record information.

15) Provide various legislative findings and declarations related to insurance and privacy.

16) Makes various other technical, non-substantive changes.

EXISTING LAW:

1) Establishes the IIPPA and provides various rights to individuals, applicants, policyholders, and insureds pursuant to the act. (Ins. Code Sec. 791 et seq.)

2) Requires an insurer to provide a notice of information practices to all applicants or policyholders in connection with insurance transactions when PI is collected only from the applicant, an insured under the policy, from public records, or from a source other than the

applicant, as specified. The required notice shall generally be in writing and state all of the following, among other things:

- Whether PI may be collected from persons other than the individual or individuals proposed for coverage.
- The types of PI that may be collected and the types of sources and investigative techniques that may be used to collect such information.
- The types of disclosures where a person's PI may be made without prior authorization, as specified.
- A description of the right to access and correct one's PI, the right to know with whom your PI was shared, the right to and know the source of the PI, and the manner in which the rights may be exercised.
- That information obtained from a report prepared by an insurance-support organization may be retained by the insurance-support organization and disclosed to other persons. (Ins. Code Sec. 791.04.)

3) Requires an insurer to clearly specify those questions designed to obtain information solely for marketing or research purposes from an individual in connection with an insurance transaction. (Ins. Code Sec. 791.05.)

4) Prohibits an insurer from utilizing its disclosure authorization form in connection with insurance transactions forms or statement which authorizes the disclosure of PI or privileged information, unless the form includes specified information, including, among other things:

   - The types of persons authorized to disclose information about the individual, and the nature of the information authorized to be disclosed.
   - The purposes for which the information is collected.
   - The length of time the authorization shall remain valid, as specified. (Ins. Code Sec. 791.06.)

5) Grants individuals, after the submission of a proper written request, the right to access recorded PI which is reasonably locatable and retrievable, as specified. Upon receipt of a proper written request, the insurer must also disclose to the individual the identity, if recorded, of those persons to whom the insurer has disclosed the individual's PI within the past two years, as specified. (Ins. Code Sec. 791.08.)

6) Requires, within 30 days of receiving a written request from an individual to correct, amend, or delete their PI, an insurer to: (1) correct, amend, or delete the PI; or, (2) notify the individual of its refusal to take the requested action and the reasons for the refusal, and inform the individual of their right to file a statement, as provided. (Ins. Code Sec. 791.09.)

7) Prohibits an insurer from disclosing and PI or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is with

the written authorization of the individual, as specified, subject a number of exceptions including the following, among others:

- To a person other than an insurer provided the disclosure is reasonably necessary to enable the person to perform a business, professional or insurance function for the disclosing insurer and the person agrees not to disclose the information further without the individual's written authorization unless the further disclosure:
    - would otherwise be permitted by this section if made by an insurer; or,
    - is reasonably necessary for such person to perform its function for the disclosing insurer.
- If the disclosure is otherwise permitted by law, or in response to a facially valid warrant, subpoena, or judicial order.
- To a person whose only use of the information will be in connection with the marketing of a product or service, so long as no medical-record information, or PI relating to an individual's character, habits, or general reputation is disclosed and the individual has been given an opportunity to indicate that he or she does not want PI disclosed for marketing purposes.
- To a medical institution or professional, as specified, or a peer review organization, as provided.
- For conducting actuarial research, as specified. (Ins. Code Sec. 791.13.)

8) Authorizes the Insurance commissioner (commissioner) to examine and investigate the affairs of every insurer in this state, issue cease and desist orders after a noticed hearing, and impose penalties for violations of cease and desist orders as follows:
    - a monetary fine of not more than $10,000 for each violation;
    - a monetary fine of not more than $50,000 if the commissioner finds that violations have occurred with such frequency as to constitute a general business practice; or,
    - suspension or revocation of an insurance institution's or agent's license if the insurance institution or agent knew or reasonably should have known it was in violation of the IIPPA. (Ins. Code Secs. 791.14, 791.17, and 791.19.)
9) Authorizes an individuals whose right to access, or right to collect, amend, or delete their PI was violated to bring an action for appropriate equitable relief in any court of competent jurisdiction. (Ins. Code Sec. 791.20.)
10) Establishes the CCPA and provides various rights to consumers pursuant to the act. Subject to various general exemptions, a consumer has, among other things:

- the right to know what PI a business collects about consumers, as specified, including the categories of third parties with whom the business shares PI, and the specific pieces of information collected about the consumer;

- the right to know what PI a business sells about consumers, as specified, including the categories of PI that the business sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold;

- the right to access the specific pieces of information a business has collected about the consumer;

- the right to delete information that a business has collected from the consumer; and

- the right to opt-out of the sale of the consumer's PI if over 16 years of age, and the right to opt-in, as specified, if the consumer is a minor; and,

- the right to equal service and price, despite exercising any of these rights. (Civ. Code Sec. 1798.100 et seq.)

11) Generally requires under the CCPA that a business subject to the CCPA do all of the following, among other things: comply with the above requirements, provide various notices to those ends, and execute various requests upon receipt of a verifiable consumer request (VCR), as specified; and provide certain mechanisms for consumers to make their lawful requests, including a clear and conspicuous link titled "Do Not Sell My Personal Information" on the business's internet homepage to enable consumers, or a person authorized by the consumer, to opt-out of the sale of the consumer's PI. (Civ. Code Sec. 1798.100 et seq.)

12) Provides that a consumer has the right to request that a business delete any PI about the consumer which the business has collected from the consumer, subject to specified exceptions. Specifically, a business or a service provider are not required to comply with a consumer's request to delete the consumer's PI if it is necessary for the business or service provider to maintain the consumer's PI in order to, among other things:

    - Complete the transaction for which the PI was collected, as specified, or otherwise perform a contract between the business and the consumer.

    - Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity.

    - Exercise or protect free speech, ensure the right of another consumer to exercise his or her right of free speech, or engage in research, as specified.

    - Comply with a legal obligation.

13) Provides, specifically, that consumers have the right to request that a business that *collects* PI about the consumer disclose to the consumer the following (and requires that the business disclose, as specified below, such information upon receipt of a VCR):

- The categories of PI it has collected about that consumer.
- The categories of sources from which the PI is collected.
- The business or commercial purpose for collecting or selling PI.
- The categories of third parties with whom the business shares PI.
- The specific pieces of PI it has collected about that consumer. (Civ. Code Sec. 1798.110; "the right to know what PI a business collects about the consumer.")

14) Provides, specifically, that consumers have the right to request that a business that *sells* the consumer's PI, or that discloses it for a business purpose, disclose to that consumer the following (and requires that the business disclose, as specified below, such information upon receipt of a VCR):

- The categories of PI that the business collected about the consumer.
- The categories of PI that the business sold about the consumer and the categories of third parties to whom the PI was sold, by category or categories of PI for each third party to whom the PI was sold.
- The categories of PI that the business disclosed about the consumer for a business purpose. (Civ. Code Sec. 1798.115; "the right to know what PI a business sells about the consumer.")

15) Grants all consumers over the age of 16 the right, at any time, to direct a business that sells PI about the consumer to third parties not to sell the consumer's PI (the right to "opt-out"). For all consumers less than 16 years of age, prohibits businesses from selling PI unless the consumer (or in the case of consumers under 13 years of age, the consumer's parent or guardian) has affirmatively authorized the sale of the consumer's PI (the right to "opt-in"). (Civ. Code Sec. 1798.120.) Requires a business, for a consumer who has opted-out of the sale of the consumer's PI, to respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's PI. (Civ. Code Sec. 1798.135.)

16) Prohibits a business from discriminating against a consumer because the consumer exercised any of the consumer's rights under the CCPA, including, but not limited to, by:

- Denying goods or services to the consumer.
- Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.
- Providing a different level or quality of goods or services to the consumer.
- Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. (Civ. Code Sec. 1798.125(a)(1), "the right to equal service and price.")

17) Specifies that nothing in the CCPA's anti-discrimination statute prohibits a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the consumer by the consumer's data, expressly authorizes a business to offer financial incentives, as specified. (Civ. Code Sec. 1798.125(a)-(b).)

18) Prohibits a business from using financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature. (Civ. Code Sec. 1798.125(b)(4).)

19) Provides various exemptions under the CCPA, including for, among other things:

- Medical information or protected health information governed by the Confidentiality of Medical Information Act (CMIA), or the Health Insurance Portability and Accountability Act (HIPAA), respectively.
- The sale of PI to or from a consumer reporting agency if that information is to be reported in, or used to generate, a consumer report as defined under specified federal regulations, and use of that information is limited by the federal Fair Credit Reporting Act (15 U.S.C. Sec. 1681 et seq.).
- PI collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), or the California Financial Information Privacy Act (Fin. Code Sec. 4050 et seq.) (Civ. Code Sec. 1798.145.)

20) Provides a limited private right of action for the CCPA's data breach section, as specified, and otherwise provides for enforcement of the act by the AG. Permits businesses to seek the opinion of the AG for guidance on how to comply with the CCPA. Includes a right to cure for businesses, if possible, as specified. (Civ. Code Secs. 1798.150 and 1798.155.)

21) Provides various definitions under the CCPA. The CCPA, of particular relevance for this bill, defines the following terms:

- "Aggregate consumer information" means information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. "Aggregate consumer information" does not mean one or more individual consumer records that have been deidentified.
- "Biometric information" means an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, 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, and sleep, health, or exercise data that contain identifying information.

- "Consumer" means a natural person who is a California resident, as defined, however identified, including by any unique identifier.

- "Deidentified" 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 business that uses deidentified information:

    - Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

    - Has implemented business processes that specifically prohibit reidentification of the information.

    - Has implemented business processes to prevent inadvertent release of deidentified information.

    - Makes no attempt to reidentify the information.

- "PI" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. PI includes specific types of information if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or *household*. These include, for example:

    - 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.

    - Characteristics of protected classifications under California or federal law.

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

    - Geolocation data.

    - Inferences drawn from any of the information identified in the definition of PI to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

  PI does not include publicly available information, as specified. Among other things, specifies that for these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, as specified. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained.

- "Pseudonymize" or "Pseudonymization" means the processing of PI in a manner that renders the PI no longer attributable to a specific consumer without the use of additional

information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the PI is not attributed to an identified or identifiable consumer.

- "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's PI by the business to another business or a third party for monetary or other valuable consideration. For purposes of the CCPA, a business does not "sell" PI when, among other things:

    - A consumer uses or directs the business to intentionally disclose, as specified, PI or uses the business to intentionally interact with a third party, provided the third party does not also sell the PI, unless that disclosure would be consistent with this title.

    - The business uses or shares an identifier for a consumer who has opted-out of the sale of the consumer's PI for the purposes of alerting third parties that the consumer has opted-out of the sale of the consumer's PI.

    - The business uses or shares with a service provider PI of a consumer that is necessary to perform a business purpose if both of the following conditions are met: (i) the business has provided notice that information being used or shared in its terms and conditions, as otherwise specified under the bill; and (ii) the service provider does not further collect, sell, or use the PI of the consumer except as necessary to perform the business purpose. (Civ. Code Sec. 1798.140.)

FISCAL EFFECT: Unknown

COMMENTS:

1) **Purpose of the bill**: This bill seeks to exempt insurers subject to the IIPPA from the CCPA and add new privacy protections to the IIPPA. This bill is author-sponsored.

2) **Author's statement**: According to the author:

    Insurers (as used here a catchall for insurers, agents/brokers, & support entities) have operated under privacy protection laws for decades. At the state level, insurers must follow privacy rules spelled out in the Insurance Information Privacy Protection Act (IIPPA) in the Insurance Code (Section 791 et seq.) and regulations adopted by the Department of Insurance (Title 10, CCR Section 2689.1 et seq.). […]

    The enactment of the CCPA will impose overlapping privacy protection laws with separate regulators/enforcers on the insurance industry. This will create regulatory conflicts and present consumers with a duplicative and confusing set of notices and disclosures, create uncertainty for consumers regarding what their rights are and what options are available to enforce them.

    The bill seeks to retain the Insurance Commissioner as the single enforcer/regulator for insurance privacy under the Insurance Code. The bill currently in print exempts insurers, agents, and insurance support organizations from the California Consumer Protection Act (CCPA) except for the CCPA data breach provision. Prohibits the sale of a minor's

information unless the insurer obtains an "opt-in". The author and sponsors are in active negotiations with a substantial group of privacy organizations regarding improvements and updates to the existing insurance law on privacy in order to make the Insurance Code privacy protections comparable to those in the CCPA.

3) **CCPA background**: Last year, the Legislature enacted the CCPA (AB 375, Chau, Ch. 55, Stats. 2018), which gives consumers certain rights regarding their PI, such as: (1) the right to know what PI that is collected and sold about them; (2) the right to request the categories and specific pieces of PI the business collects about them; and (3) the right to opt-out of the sale of their PI, or opt-in in the case of minors under 16 years of age. The CCPA was the byproduct of compromises made between business interests on the one side, and consumer and privacy interests on the other, to provide a legislative alternative to a ballot initiative on the same subject.

   The CCPA provides a number of exemptions from the act (both in whole and in part), designed to generally to facilitate the disclosure of information where such sharing is required to satisfy the purpose for which the consumer shared their information in the first place. For example, the definition of "sale" excludes PI that is necessarily shared with a service provider to perform a business purpose if the service provider does not further collect, sell, or use the PI except as necessary to perform the business purpose. (Civ. Code Sec. 1798.140(t).) Business purposes include, for example:

   - auditing related to a current interaction with the consumer, as specified;

   - detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity; and,

   - performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, or providing similar services on behalf of the business or service provider. (Civ. Code Sec. 1798.140(d).)

   The CCPA also exempts businesses and service providers from the obligation of deleting a consumer's PI, as specified, if the business or service provider maintain the PI in order to:

   - Complete the transaction for which the PI was collected, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business's ongoing business relationship with the consumer, or otherwise perform a contract between the business and the consumer.

   - Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

   - Debug to identify and repair errors that impair existing intended functionality.

   - Exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law.

   - Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the

businesses' deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

- To enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

- Comply with a legal obligation.

- Otherwise use the consumer's PI, internally, in a lawful manner that is compatible with the context in which the consumer provided the information. (Civ. Code Sec. 1798.105.)

In addition, the CCPA does not apply to certain types of information at all. These are generally types of information that fall under a privacy protective scheme that accounts for the specific type of information sharing that is required for that particular industry. For example, medical information, as governed by California's Confidentiality of Medical Information Act (CMIA), and, similarly, protected health information under the federal Health Insurance Portability and Accountability Act (HIPAA) are not subject to the CCPA because the sharing of patient information with healthcare providers and other covered entities is necessary in the healthcare setting. CMIA also guarantees privacy protections with its robust enforcement scheme, including a private right of action.

Of particular relevance to the insurance industry, the CCPA excludes PI collected, processed, sold or disclosed pursuant to two financial privacy laws: the Gramm-Leach-Bliley Act (GLBA) and the California Financial Information Privacy Act. This bill now, in contrast to the CCPA's existing exemptions which generally exempt privacy protected information, and not entities, seeks to exempt insurance institutions, agents, insurance-support organizations, or insurance transactions subject to the IIPPA from the CCPA.

A coalition of insurance agencies and associations writes in support:

> The industry as a whole supports robust regulation of personal information and we have long been diligent stewards of customers' highly sensitive personal information. We have managed consumers' sensitive medical and financial information appropriately far before it became "data."
>
> The industry has supported the enactment of federal and state laws and regulations that provide a complex, broad and rigorous regulatory framework that has long required insurers to protect both the privacy and the security of their customers' personal information. […]
>
> When the Legislature passed the CCPA, it failed to acknowledge California Insurance Code. Sec. 791 which is the Insurance Information and Privacy Protection Act (IIPPA). This statute has long governed how the insurance industry protects consumers' information and includes robust requirements very similar to the CCPA. […]
>
> If there are additional consumer protections needed beyond those provided in the IIPPA, a much better solution would be to clarify such issues in the IIPA. Trying to reconcile the CCPA with a long standing and well-vetted insurance-specific law will result in

foreseeable legal conflicts, and jeopardize the critical balance achieved in current privacy and security laws applicable to and strongly supported by insurers.

4) **Privacy Protections under the IIPPA**: California Insurance Code Sections 791 - 791.27, the IIPPA, provide protections for one's personally identifiable information, which is generally provided to an agent, broker, or insurance company in order to apply for insurance or submit a claim. These entities must provide individuals with a "Privacy Notice" that describes the entities' practices and policies regarding privacy, the kind of information collected in connection with an application for insurance, submission of a claim, or other insurance transaction; how and with whom personally identifiable information will be shared, and rights to restrict that sharing.

   The IIPPA is enforced by the Insurance commissioner (commissioner), who has the author to issue cease and desist orders for violations of the act. (Ins. Code Sec. 791.17.) Any person who violates a cease and desist order may be subject to a fine of not more than $10,000 for each violation, or up to $50,000 if the commissioner finds that violations have occurred with such frequency as to constitute a general business practice. (Ins. Code Sec. 791.19.)

   While on their face, many of the protections provided in the IIPPA look similar to those provided in the CCPA, they are far from duplicative. For example, individuals have the right to access the PI collected about them under both laws. The IIPPA, however, requires that the requested information is "reasonably locatable and retrievable" by the insurer. The insurer additionally only has to disclose the identity of the additional persons to whom they disclosed the PI "if recorded." (Ins. Code Sec. 791.08.) No such exceptions apply in the CCPA.

   Similarly, the IIPPA gives individuals the right to delete, correct, and amend their PI. Unlike the CCPA, however, which explicitly lists why a business would not have to comply with a request to delete information (*e.g.*, including to complete a transaction, detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or to comply with a legal obligation), the IIPPA only requires that the insurer notify a consumer of the reason they are refusing to delete or correct the PI. The potential numbers of reasons an insurer could refuse to accommodate an individual's request are seemingly endless. If an insurer refuses to delete, correct, or amend an individual's information, they must inform the individual that he or she can file a statement setting forth what information the individual thinks is correct. In any subsequent disclosure of the PI, the insurer would be required to disclose the statement as well. (Ins. Code Sec. 791.09.) As manner by which an individual can control the PI collected and sold about them, this remedy pales in comparison to what the CCPA provides.

   The IIPPA also lets individuals opt-out of the sharing of their PI for marketing purposes. Unfortunately, the IIPPA does not define "marketing purposes," and so it is not clear how broad (or narrow, as the case may be) this right is. The CCPA, by contrast, permits a consumer to opt-out of information sharing much more broadly, subject to specified exceptions discussed in Comment 3, above.

   In opposition to this bill, the Consumer Attorneys of California write:

   > As a baseline, when other privacy laws have established overlap with the CCPA our position has been that the law that is more consumer privacy protective should be the

prevailing standard. Article 1, Section 1 of the California Constitution has established privacy as an inalienable right for every California citizen. The California Consumer Privacy Act has established important mechanisms for Californians to realize those rights. Specifically, the CCPA provides several rights, including:

- Know all of the data a business collects about you and receive it in a portable format.
- Delete data you've given to a business.
- Have the right to say no to the sale of your information to third parties.
- Hold companies accountable in the event they didn't take reasonable steps to keep your information safe.

These rights, as they have been established by the CCPA, are not mirrored in the IIPPA and there are areas where the rights do not overlap. The CCPA contains important provisions that ensure that, where compliance with the CCPA would interfere with other legal compliance, businesses can continue to operate and comply with federal, state and local laws.

5) **Efforts to incorporate CCPA's privacy protections into IIPPA fall short**: Recent amendments seek to enhance privacy protections in the insurance industry. Specifically, as recently amended, this bill would require insurers to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards for the protection of policyholder information. Additionally, recent amendments incorporate a number of concepts from the CCPA into the IIPPA, including, among others:

- Incorporating various definitions from the CCPA including the definitions for "aggregate consumer information," "biometric information," "consumer," "deidentified," "pseudonymize," and "PI."
- Updating various disclosures and requiring insurers to provide a notice of information practices, including the categories of PI that may be collected and the purposes for which the categories of personal information may be used.
- Allowing the unauthorized sharing of PI for the purpose of conducting research studies performed by nonaffiliated entities, as specified.
- Allowing policyholders to request and receive a copy of their PI, in a readily useable format that can be transferred to another entity.
- Prohibiting insurers, for all insureds less than 16 years of age, from selling the insured's PI, unless the insured (or in the case of insureds under 13 years of age, the insured's parent or guardian) has affirmatively authorized the sale of the insured's PI.
- Providing that an insurer shall not unfairly discriminate against an applicant or policyholder because that applicant or policyholder has opted-out from the disclosure of nonpublic PI. Defines "unfairly discriminate" to include denying an applicant or

policyholder a product or service because the applicant or policyholder has refused to authorize disclosure of nonpublic personal information.

The Civil Justice Association of California (CJAC) writes in support, "AB 981 is designed to prevent needless duplication of privacy rights in the insurance context between the longstanding Insurance Information Privacy Act [IIPPA] and the newly-enacted California Consumer Privacy Act (CCPA). For decades, insurance consumers have been protected by the provisions of [IIPPA], conferring rights including disclosure of collection and use of personal information, deletion or amendment of consumer information, and more. These rights are largely duplicative of rights granted to consumers broadly in CCPA."

While attempts to incorporate the protections found in the CCPA in the IIPPA are apparent, the recent amendments fall short of the protections granted under the CCPA for a variety of reasons. For example, incorporating definitions does not, in and of itself, necessarily increase privacy protections if those definitions apply to protections that are arguably not that strong to begin with. The IIPPA has quite a few broad exemptions to the prohibition against sharing individuals' PI absent their consent. In addition, the definitions, in many respects, are not identical to those in the CCPA. For example:

- The definition of "consumer" reflects the definition of that word from the March 25, 2019, version of AB 25. That bill has been subsequently amended and will likely be amended again as it continues to move through the legislative process.

- The definition of "PI" appears to mirror the definition of that term provided in the CCPA, with the exception of "household" missing from the definition. The elimination of this term from the definition of PI creates a much weaker definition of PI, offering less protection to individuals under AB 981 than that which is provided under the CCPA.

Furthermore, as currently in print, AB 981 would allow the sharing of PI without an insured's consent for specified research. There are two problems with this provision when compared to CCPA. First, the CCPA only provides that a business need not *delete* a consumer's PI when it is being used for specified research. A consumer can still opt-out of the sharing of their PI for research purposes under the act. The exemption in AB 981 is much more expansive and less protective of privacy. Second, the definition of "research" in AB 981, while similar to the definition in the CCPA, leaves out an important element. Namely, in CCPA, research cannot be for any commercial purpose. This restriction is conspicuously absent from AB 981.

Next, similar to the data portability element in the CCPA, AB 981 would give a policyholder the right to request and receive a copy of the policyholder's PI from an insurer in a readily usable format that can be transferred to another entity. Unlike the CCPA, which gives any consumer who has had contact with a business the right to their PI in a portable and readily useable format, AB 981provides a more narrow right and limits the right of portability to policyholders. This effectively excludes insured family members (who are on the policy, but not the policyholder), applicants, and any other individual about whom the insurer has collected PI (perhaps potential clients or former insureds). Similarly, the prohibition on selling minor's PI absent an authorization, as specified, is limited to *insureds*. This would exclude applicants, former insureds, and other minors about whom the insurer has collected PI.

Finally, AB 981 seeks to incorporate an anti-discrimination provision in a nod to the anti-discrimination provision in the CCPA. In contrast to this bill, the CCPA, prohibits a business from discriminating against a consumer because the consumer has exercised *any* of their rights provided by the CCPA. That provision prohibits discrimination by denying goods or services, charging different prices for the goods or services, or providing a different level or quality of services. AB 981, however, would only prohibit an insurer from *unfairly* discriminating against an applicant or policyholder because that applicant or policyholder has opted out from the disclosure of nonpublic PI.

This provision raises a number of significant concerns. First, it is limited to policyholders and applicants. This excludes many insureds and other individuals about whom the insurer may have PI. It is also limited to a policyholder's choice to opt-out of the disclosure of their PI, and does not offer protections if the policyholder exercises any of their other rights under the IIPPA and/or AB 981, such as the right to access PI, the right to delete PI, the various rights to disclosures, and the right to data portability. AB 981 would describe "unfair discrimination" as denying an applicant or policyholder a product or service, whereas the CCPA authorizes certain non-discriminatory incentive, which can take the form of discounts, incentives, or providing different levels of service. Notably, the CCPA prohibits any offering from being unjust, unreasonable, coercive, or usurious in nature. Finally, it is important to keep in mind that the right of privacy is a constitutional right in California. As a matter of public policy it is troubling to imply that a person can be *fairly* discriminated against in their constitutionally-held rights.

6) **As evidenced by recent amendments, the insurance industry is willing to comply with concepts in the CCPA, but express concern at the prospect of having two regulators**: To a large extent, the existing exemptions in the CCPA give industry an ability to disregard provisions of the CCPA that conflict with obligations required by other laws, such as the IIPPA. As noted by the Center for Public Interest Law at the University of San Diego School of Law in opposition:

> [R]espectfully, why an exemption for the whole industry when the CCPA itself could be amended in ways that address any unexpected implementation issues specific to the insurance industry. The author did not demonstrate an aversion to nuanced amendments. If he had, we would not see a provision like this in the CCPA, offering a broad exemption:
>
> > 1798.105. (d) A business or a service provider shall not be required to comply with a consumer's request to delete the consumer's personal information if it is necessary for the business or service provider to maintain the consumer's personal information in order to:
> >
> > ***(9) Otherwise use the consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information.***
>
> Surely, this highlighted language is sufficient to address almost every conceivable insurance-related use of personal information. If not, then a discussion should be had about amending it or amending some other part of the CCPA. [Emphasis in original.]

Additionally, the CCPA provides that the "obligations imposed on businesses by this title shall not restrict a business's ability to [c]omply with federal, state, or local laws." (Civ. Code Sec.1798.145(a).) As noted above in Comment 3, there are also a number of exceptions that allow for the sharing of PI in order to complete business transactions. Californians for Consumer Privacy raises this point in their letter of opposition:

> [T]he CCPA contemplates the need for data sharing to perform business functions. As a result, Civil Code Section 1798.140 (d) defines "business purpose," which allows a business to share a consumer's data for defined operational purposes and from which the consumer cannot opt-out. It is unclear why providing this right to consumers creates conflicts with the administration of insurance.

Many insurance agencies and associations support this bill, in part because they do not wish to be subject to enforcement actions from two regulators: the insurance commissioner and the AG. For example, Insurance Services Office, Inc. writes in support:

> The California Department of Insurance has nearly 40 years' experience enforcing the [IIPPA] to ensure consumer privacy protections are in place. Subjecting insurers and their support organizations to two privacy laws will create confusion and inefficiencies that can negatively impact insurance consumers. Further, it may be unclear which agency would regulate the insurance industry in such matters.

Allstate Insurance Company, also writes in support that "[w]e agree that insureds are better off with one consistent regulator – the Insurance Commissioner – than by having to seek redress for possible privacy issues from a second regulator – the Attorney General."

In other words, the insurance industry has not argued that compliance with the CCPA is unattainable. They instead argue that they have a privacy protective scheme under the IIPPA. Again, creating new privacy protections in the IIPPA, even if seemingly modeled after the CCPA, is not as protective of privacy as the CCPA, itself, as discussed in Comment 5 above. Furthermore, as an industry, insurers are accustomed to following multiple statutory schemes, as evidenced by their compliance with HIPAA (for medical insurers) and GLBA (for insurance more generally). Staff notes that information governed under either of these statutory schemes is exempted from the CCPA, further calling into question the need for a broad exemption for the insurance industry. Additionally, having rights that appear identical on the surface, but are fundamentally different in practice, could be confusing for Californians trying to control the dissemination of their PI and exercise their rights. The IIPPA also lacks a comparable enforcement scheme by which individuals rights can be enforced. As noted by Californians for Consumer Privacy in opposition:

> The CCPA establishes new enforcement standards, including rights for California consumers to hold companies accountable in the event they do not take reasonable steps to keep a consumer's information safe. The CCPA also provides three safe harbors from this liability - if a company takes steps to ensure reasonable security measures, encrypts information, or redacts information. While we appreciate that AB 981 has been amended to not cover the data breach provisions, the CCPA also provides enforcement authority to the California Attorney General and specifies the monetary penalty thresholds per violation. The IIPPA requires the Insurance Commissioner to conduct an administrative hearing to review alleged violations of the law and issue a cease and desist letter if he or

she determines that an insurance institution, agent, or insurance support organization has violated the law. The IIPPA authorizes the Insurance Commissioner to impose penalties only if the insurance institution, agent, or insurance support organization *continues* to violate the law after receiving the cease and desist letter, with penalties not exceeding $50,000 if the commissioner finds that violations have occurred with such frequency as to constitute a general business practice. The enforcement mechanisms are materially different and would result in significantly lower penalties under the IIPPA should there be a significant violation of consumers' privacy rights."

Given the existing exemptions in the CCPA, especially the exemption for information collected, processed, sold, or disclosed pursuant to GLBA, the insurance industry arguably does not need an exemption from the CCPA. That being said, there are two provisions in the CCPA that could create issues for insurers if the existing exemptions did not apply: the right to opt-out of the sale of one's information, and the right to delete one's information. These rights could (again, if existing exemptions did not apply), complicate the process by which an insurer is able to provide insurance products and services requested by the consumer. Insurance is a necessity in modern life upon which we all depend. To the extent that the CCPA may create confusion for insurers in the delivery of insurance products and services, the Committee may wish to provide absolute clarity with the following suggested amendment, if it were to approve this bill. This amendment would provide that, to the extent that it is necessary to retain or sell a consumer's PI to provide an insurance service or product that is requested by a consumer, the right to opt-out of the sale of one's information and the right to delete do not apply.

Suggested amendment:

Page 5, strike lines 26-29.

Create a new subdivision (f) in 1798.145 to read: "*Sections 1798.105 and 1798.120 shall not apply to the extent it is necessary to retain or sell a consumer's personal information to complete an insurance transaction, as defined in section 791.02(m) of the Insurance Code, for a product or service that has been requested by the consumer*."

Renumber subsequent subdivisions accordingly.

7) **Related legislation**: AB 25 (Chau) seeks to clarify the CCPA's definition of consumer and how businesses may comply with a consumer's request for specific pieces of information in a privacy protective manner under the CCPA. This bill is pending hearing in this Committee.

AB 288 (Cunningham) seeks to establish laws governing "social media privacy" separate and apart from the CCPA's existing requirements for such companies that meet the "business" definition thresholds identified in the CCPA. Specifically, the bill would require a social networking service, as defined, to provide users that close their accounts the option to have the user's "personally identifiable information" permanently removed from the company's database and records and to prohibit the service from selling that information to, or exchanging that information with, a third party in the future, subject to specified exceptions. The bill would require a social networking service to honor such a request within a commercially reasonable time. The bill would authorize consumers to bring private right of action for a violation of these provisions, as specified. This bill has been referred to this Committee.

AB 523 (Irwin) seeks to address the sale of geolocation information by certain businesses, separate and apart from the CCPA's existing requirements and restrictions governing companies that meet the "business" definition thresholds identified in the CCPA and seek to sell their consumers' PI (which the CCPA defines to include geolocation information). This bill is pending hearing in the Assembly Communications and Conveyance Committee.

AB 846 (Burke) seeks to replace "financial incentive programs" provisions in the non-discrimination statute of the CCPA with an authorization for offerings that include, among other things, gift cards or certificates, discounts, payments to consumers, or other benefits associated with a loyalty or rewards program, as specified. This bill is pending hearing in this Committee.

AB 873 (Irwin) seeks to narrow the CCPA's definitions of "PI" and "deidentified" and to revise the CCPA's existing provision that prohibits the act from being construed to require a business to reidentify or otherwise link information that is not maintained in a manner that would be considered PI. This bill is pending hearing in this Committee.

AB 874 (Irwin) seeks to broaden the definition of "publicly available" for purposes of the PI definition, which excludes "publicly available" information. The bill would also correct a drafting error in the definition of "PI" to clarify that PI does not include deidentified or aggregate consumer information. This bill is pending hearing in this Committee.

AB 1035 (Mayes) seeks to require, under the Data Breach Notification Law, a person or business, as defined, that owns or licenses computerized data that includes PI to disclose any breach of the security of the system within 72 hours following discovery or notification of the breach, subject to the legitimate needs of law enforcement, as provided. This bill is pending hearing in this Committee.

AB 1138 (Gallagher) seeks to prohibit a person or business that conducts business in California, and that operates a social media website or application, from allowing a person under 16 years of age to create an account with the website or application unless the website or application obtains the consent of the person's parent or guardian before creating the account. This bill is pending hearing in this Committee.

AB 1146 (Berman) seeks to expand the CCPA exemptions to expressly exclude from the CCPA vehicle information shared between a new motor vehicle dealer and the vehicle's manufacturer, if the information is shared pursuant to, or in anticipation of, a vehicle repair relating to warranty work or a recall, as specified. This bill is pending hearing in this Committee.

AB 1355 (Chau) seeks to address a drafting error in the definition of PI to clarify that it does not include deidentified or aggregate consumer information. This bill is pending hearing in this Committee.

AB 1395 (Cunningham) seeks to prohibit a smart speaker device, as defined, or a specified manufacturer of that device, from saving or storing recordings of verbal commands or requests given to the device, or verbal conversations heard by the device, regardless of whether the device was triggered using a key term or phrase. This bill is pending hearing in this Committee.

AB 1416 (Cooley) seeks to expand the CCPA exemptions to specify that the act does not restrict a business's ability comply with any rules or regulations. The bill would also expand the CCPA existing exemptions, which already include that the act does not restrict a business's ability to exercise or defend legal claims, to instead specify that the act does not restrict a business's ability to collect, use, retain, sell, authenticate, or disclose PI: (1) in order to exercise, defend, or protect against legal claims; (2) in order to protect against or prevent fraud or unauthorized transactions; (3) in order to protect against or prevent security incidents or other malicious, deceptive, or illegal activity; (4) in order to investigate, report, or prosecute those responsible for protecting against fraud, unauthorized transactions, and preventing security incidents or other specified activities; or, (5) for the purpose of assisting another person or government agency to conduct the aforementioned activities. This bill is pending hearing in this Committee.

AB 1564 (Berman) would revise a requirement in the CCPA for businesses to make available to consumers "two or more designated methods" for submitting requests for information to be disclosed pursuant to specified provisions of the CCPA, including, at a minimum, a toll free telephone number and, if the business maintains an internet website, a website address. This bill is pending hearing in this Committee.

AB 1760 (Wicks) would restate the CCPA rights using similar terminology, expand those existing CCPA rights to include new rights, and replace the "opt-out" rights of consumers 16 years and older with an "opt-in" right, among other things. This bill is pending hearing in this Committee.

8) **Prior legislation**: AB 375 (Chau, Ch. 55, Stats. 2018) *See* Comment 3.

SB 1121 (Dodd, Ch. 735, Stats. 2018) *See* Comment 3. This bill ensured that a private right of action under the CCPA applies only to the CCPA's data breach section on and not to any other section of the CCPA, as specified, corrected numerous drafting errors, made non-controversial clarifying amendments, and addressed several policy suggestions made by the AG in a preliminary clean-up bill to AB 375.

9) Double-referral: This bill was double referred to the Assembly Insurance Committee were it was heard on April 3, 2019, and passed out on a 14-0 vote.

REGISTERED SUPPORT / OPPOSITION:

Support

ACLHIC
Allstate Insurance Company
American International Group, Inc.
American Property Casualty Insurance Association
Association Of California Life & Health Insurance Companies
Automobile Club Of Southern California
California Association Of Health Underwriters
Civil Justice Association Of California
CSAA Insurance Group
Independent Insurance Agents & Brokers Of California, Inc.
Insurance Services Office, Inc.

Liberty Mutual Insurance
Mercury General Corporation
NAMIC
National Association Of Insurance And Financial Advisors - California
Nationwide Mutual Insurance Company
Pacific Association Of Domestic Insurance Companies
Personal Insurance Federation Of California
Sentry Insurance, a Mutual Company
State Farm Los Angeles
State Farm Mutual Automobile Insurance Company
Travelers Companies Inc. And Subsidiaries
Zenith Insurance Company

Opposition

Californians For Consumer Privacy
Center For Public Interest Law/Children's Advocacy Institute/University Of San Diego
Consumer Attorneys Of California
Consumer Watchdog

Analysis Prepared by: Nichole Rapier / P. & C.P. / (916) 319-2200