Statement

Insurance Association of Connecticut

Government Administration and Elections Committee

March 25, 2019

SB 1108 - An Act Concerning Consumer Privacy

I am Eric George and I am the President of the Insurance Association of Connecticut (the "IAC"). The IAC strongly opposes SB 1108, An Act Concerning Consumer Privacy.

As well-intended as SB 1108 is, it is tremendously far-reaching and is based on a recent California statutory scheme that was enacted (1) with nearly no debate, (2) in a hyper-shortened time-period that allowed for no significant public review, and (3) which is currently being strongly reconsidered for substantive amendment.

Please recognize that the issue of consumer data and information security are paramount to the insurance industry. As the stewards of such information, it is our mission to protect and maintain the integrity of this data and information. And the insurance industry is one of the most highly regulated and scrutinized industries in Connecticut. The Connecticut Department of Insurance acts as a watchful guardian of the public's data and information.

Please know that the IAC is a member of both the American Property and Casualty Insurers of America (APCIA) and the American Council of Life Insurers (ACLI). The IAC, APCIA and ACLI have a number of common members. The IAC fully endorses the APCIA's and ACLI's testimonies on this legislation, and they are each attached hereto at Attachment 1 and Attachment 2, respectively.

Thank you for your consideration of our comments. The IAC strongly urges this Committee to reject SB 1108.

Attachment 1

APCIA Testimony

STATEMENT

AMERICAN PROPERTY CASUALTY INSURANCE ASSOCIATION (APCIA)

S.B. No. 1108 – AN ACT CONCERNING CONSUMER PRIVACY

GOVERNMENT ADMINISTRATION AND ELECTIONS COMMITTEE

March 25, 2019

The American Property Casualty Insurance Association (APCIA)[1] appreciates the opportunity to comment on Senate Bill No. 1108, An Act Concerning Consumer Privacy. With members comprising nearly 60 percent of the U.S. property casualty insurance market, APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association.

Consumer privacy and data security are priority issues for the insurance industry and insurers devote considerable resources to protect data, information systems, and consumer trust. While APCIA agrees that these issues must be afforded top priority, we also believe that efforts in this regard must be carefully tailored to ensure that they are workable, effective, do not pose insurmountable burdens for businesses and do not result in unintended negative consequences for businesses and consumers. APCIA opposes this legislation because, while well intentioned, we believe that it is overly broad and may result in highly problematic unintended consequences.

---

[1] Effective January 1, 2019, the American Insurance Association (AIA) and the Property Casualty Insurers Association of America (PCIAA) merged to form the American Property Casualty Insurance Association (APCIA). Representing nearly 60 percent of the U.S. property casualty insurance market, APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers. APCIA represents the broadest cross-section of home, auto, and business insurers of any national trade association. APCIA members represent all sizes, structures, and regions, which protect families, communities, and businesses in the U.S. and across the globe.

The insurance industry has been subject to privacy statutes and regulations for over two decades. Insurers are "financial institutions" for the purpose of the Gramm-Leach-Bliley Act (GLBA) and all 50 states and the District of Columbia have adopted regulations implementing GLBA and/or have statutes consistent with and, in some instances, stricter than GLBA. In addition to GLBA, Connecticut insurers are subject to Conn Gen. Stat. §§38a-975 et seq., the "Connecticut Insurance Information and Privacy Protection Act" and Conn. Agencies Regs. §§38a-8-105 et. Seq., "Privacy of Consumer Financial Information." This long-established privacy landscape appropriately balances consumer protection with the legitimate business needs of all parties to an insurance transaction.

SB1108 raises significant concerns regarding unnecessary obstacles and potential unintended consequences that will overturn this long established privacy framework. Additionally, even if the General Assembly was inclined to move forward with legislation of this nature, APCIA would submit that pursuing this legislation, which appears to be based on the California Consumer Privacy Act (CCPA), is premature because the CCPA is still in the process of being implemented. Regulations implementing the CCPA have not been finalized and numerous bills are currently pending in California to remedy problems with the hastily passed CCPA. Given that the CCPA is still a work in progress in many respects, it would not seem to be wise to be duplicating a law around which there continue to be many implementation questions and problems. Additionally, requiring businesses to comply with a myriad of different states' versions of this law would make the already unworkable CCPA even more impossible from a compliance standpoint. Accordingly, Connecticut should not consider moving forward with duplicating the flawed CCPA until its provisions and implementing regulations have been finalized. Even once the CCPA provisions and regulations are finalized, Connecticut should wait to see how the provisions are working in the real world prior to implementing a similar law so as to make sure that the law is workable from a business and consumer standpoint.

In addition to these general points in opposition to this legislation, the following is a non-exclusive list of specific concerns supporting our opposition to this legislation.

Consumer

Fundamentally, it is important to remember that this is a consumer issue and the scope of the bill and definitions included therein should be narrowly tailored to meet that objective. For example, employee data and data related to a commercial transaction should be exempt. As currently defined, the term "consumer" is broad enough to include any natural person who is a Connecticut resident. "Consumer," therefore, could include an individual acting in his or her commercial or employment capacity – not only his/her personal capacity – such as an insurance agent, shareholder, vendor, or commercial insured. This is particularly concerning given the breadth of the definition of "personal information." Consider, for example, commercial insurance policies where

the insurer may need to have the personal information of individuals working at a business to process a corporate executive or professional liability policy, employee information for workers' compensation, processing of a commercial auto or commercial general liability claim, or personal information about an individual principal to issue a commercial surety or fidelity bond, etc. Implementing and complying with SB1108 opt-out and disclosure obligations could unnecessarily stall or even prevent a commercial transaction from moving forward. Accordingly, APCIA believes that the definition of "Consumer" should be significantly narrowed so as to eliminate any ambiguity and appropriately narrow the scope to personal consumer transactions.

Personal Information

APCIA also believes that the scope of the definition of "personal information" in this bill is far too inclusive. For example, inclusion of information "capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household" is very problematic. The list could be exhaustive in this context, to include even pseudonymized information. In addition, the household information could be so tangential that there is no ability to associate a single individual with the information, yet it is considered "personal information" under a strict reading.

We also question how an Internet Protocol Address (IP Address) can be considered "personal information" or a "unique identifier." Given the sharing restrictions and notification obligations, considering an IP Address personal information could actually harm consumers rather than provide any consumer benefit.

Sale

The current definition of sale includes "other valuable consideration." From a property/casualty insurance perspective this is particularly concerning as it has the potential to impact important information sharing arrangements in the context of fraud prevention, claims handling, underwriting, and other necessary business functions. For instance, insurers participate in contributory databases to share information to prevent fraud and material misrepresentations. These are critical functions that benefit not only consumers but society. In addition, a 3rd party may require personal information to perform a necessary business function that they then de-identify and aggregate for their own purposes.

Privileged Information

APCIA questions the protections SB1108 provides for confidential and privileged information. Currently, the only protection is a limited exemption tied to an "evidentiary privilege." This is extremely narrow and creates a high burden to meet with multiple complex legal issues. The exemption does not account for information of a sensitive or confidential nature. There also has to be a Connecticut evidentiary rule that is applicable negating the possibility of cross border litigation needs and suggests that a proceeding must already be in place. Hence, an individual that might be contemplating litigation, or even fraud, is able to obtain information from the business

to prepare their case. The Connecticut legislature has already recognized that such disclosures are not in the public interest in the insurance context. Conn Gen. Stat. §§38a-975 et seq., the Insurance Information Privacy Protection Act, has a privilege exemption that applies when there is reasonable anticipation that a claim or criminal proceeding will be filed.

Notice

A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. APCIA believes there are potential unintended consequences that will only serve to confuse and frustrate consumers. For instance, consumers may receive multiple notifications for a single transaction, because the obligation is not limited to the business that has the direct relationship with the consumer. Additionally, businesses should be provided flexibility to meet this notification obligation. Given the broad scope of recipients it may be difficult to identify all individuals in an efficient and timely manner.

Production of Personal Information

There are multiple sections of SB1108 that require information be disclosed in a readily useable format upon receipt of a verifiable consumer request. How is a business to determine under which section the verifiable consumer request has been made? What are the practicable distinctions between these sections? If a business discloses the "incorrect" information, would a business be liable for failure to distinguish between these similar portions of the statute? Clarification on the responsibilities of businesses in responding to verifiable consumer requests is necessary for businesses to comply properly with CCPA's requirements.

GLBA Exemption

SB1108 contains a GLBA exemption that is based on the personal information collected, processed, sold or disclosed pursuant to GLBA. Of significance, the exemption only applies if there is a conflict between SB1108 and GLBA causing a business to have to make the difficult decision as to where there is a conflict and if the enforcing regulator or attorney general will agree. Further, without an entity-based exemption, the differences in the definitions of "personal information" in GLBA and SB1108 establishes a legal framework of competing obligations that could, for instance, necessitate multiple privacy notices ultimately confusing consumers. It is critical that this exemption be changed to an entity based exemption and eliminate the "in conflict" language. The GLBA exemption could read as follows: "Section 1 to 18, inclusive, of this act shall not apply to a business or an affiliate of a business subject to, or governed by, or personal identifying information processed, collected, used, sold, or disclosed under the Gramm-Leach-Bliley Act (Pub. L. No. 106-102) and implementing regulations."

Operational Effective Date

It will take a company significantly longer than a year to first determine how to comply with unworkable restrictions in SB1108 and second to implement the requirement. We recommend a five-year implementation timeframe.

The information above provides just a few illustrations as to why SB1108 may create unintended consequences that could potentially harm rather than benefit consumers. For these reasons we oppose SB1108.

For the foregoing reasons, APCIA urges your Committee NOT to advance this bill.

Attachment 2

ACLI Testimony

TESTIMONY OF THE AMERICAN COUNCIL OF LIFE INSURERS

before the
Government Administration & Elections Committee March 25, 2019

Senate Bill 1108 – An Act Concerning Consumer Privacy

Chair Fox and Chair Flexer and distinguished members of the Government Administration & Elections Committee, the American Council of Life Insurers (ACLI) appreciates the opportunity to offer the following statement on Senate Bill 1108 – An Act Concerning Consumer Privacy. ACLI members are the leading writers of life insurance, annuities, disability income insurance, long-term care insurance and supplemental benefit insurance here in Connecticut and across the country. We respectfully submit the following testimony in *strong opposition* to Senate Bill 1108.

Consumers deserve and expect that the personal information they have entrusted to businesses will be kept confidential and secure. In line with that premise, insurers have long been the diligent stewards of personal information. We have appropriately managed consumers' sensitive medical and financial information far before it became "data" and was monetized by the technology sector. While governance around the use of data is very new on the tech side, the financial service industry has robust regimen for the use of personal data. Insurers' enduring commitment to safeguarding customer information is the force behind our work to establish what has become a comprehensive federal and state regulatory framework governing the use and disclosure of personal information. Under these auspices, existing Connecticut standards currently provide protections, enforcement and remedies regarding confidentiality and disclosure of consumers' personal insurance data similar to those proposed in the bill before you today.

Connecticut has been on the forefront of the protecting the use of personal information by financial institutions with the adoption of a comprehensive list of statutes and regulations, including, among others: *the Connecticut Insurance Information and Privacy Protection Act (CT Gen. State. Ann Sec. 36a-975); the Privacy of Consumer Financial Information (CT ADC Se. 38a-8-105);* and*, the Safeguarding of Customer Financial Information (CT ADC Sec. 38a-8-124).*

While we support a rigorous regulatory framework for the appropriate use of sensitive personal information, ACLI strongly opposes the adoption of divergent state-by-state requirements and restrictions concerning data privacy. Data in this day and age is not static and, unlike paper records, does not reside permanently in any one place. Increasingly data is stored on cloud-based platforms

which are not confined by state borders. A patchwork quilt of divergent state privacy laws will create complexity and confusion for both consumers and companies. This confusion will unavoidably lead to nonsensical data processes and less security and certainty around the use of personal information.

The bill before you today is modeled after the California Consumer Privacy Act of 2018. The California law was passed in 4 days, behind the scenes, with virtually no public input. It was rushed and the result is evident. There are numerous provisions that do not make logical sense and are nearly impossible to implement. Some of the purported consumer protection disclosure requirements in the proposal will render consumers' personal information even more vulnerable. And the severe impact to entities forced to completely overhaul their business practices in order to comply with the law was not given much, if any, thought. As a result, there are over 20 bills currently before the California legislature this session to fix the law. It is public policy chaos.

While we urge you not to pass any law at this time, if you are determined to proceed, we recommend that the current state and federal regulatory framework for safeguarding consumers' personal information be harmonized with any legislation that is enacted in order to avoid any unnecessary conflicting or overlapping requirements.

We direct our next comments to the numerous concerns with provisions of Senate Bill 1108. Due to the rushed timeframe between the bill's introduction and the public hearing on this comprehensive proposal, we are not able to include an exhaustive list of the problems but here are some of our top concerns:

The definition of "consumer" is overly broad. It could include individuals with no business relationship with company including employees. The definition also impacts business to business relationships. Moreover, it is inconsistent with the definition of consumer under existing Connecticut requirements including *the Privacy of Consumer Financial Information (CT ADC Se. 38a-8-105(7)).* The current broad definition of "consumer" will have a negative effect on commerce and millions of dollars in compliance costs.

The definition of "personal information", which underlies most of the bill's new consumer rights and new requirements for businesses, is also overly broad. The definition includes information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a consumer or household. Due to the complexity of the requirements relating to sale of personal information, the bill's possible impact on other ordinary insurance business arrangements or activities, such as, for example, joint marketing agreements, or an agent's sharing with an insurer of a proposed insured's personal information on an application for an insurance policy will be impacted.

It should be made clear in Sections 2 and 4 that companies only need to provide *categories* of personal data rather than specific pieces of data. Providing specific pieces of information such as a consumer's social security number or driver's license number in response to a request creates risk to the consumer's information. These provisions would require businesses to maintain records that directly identify individuals which would undermine privacy. Moreover, investigating and correlating each specific piece of data with an identifiable person is unfeasible.

SB 1108 contains a number of different provisions relating to a business not being required to reidentify or retain information in order to comply with the requirements of the law. The

provisions are inconsistent, and the confusion will have the perverse adverse effect of discouraging companies from deidentifying personal data. An example of this is the exception in Section 11(i) which applies to all sections of the law but only to reidentification, thus by implication suggesting that more information must be collected in order to comply with the other sections of the bill's complicated requirements related to partially identified data. Businesses should not be required to re-identify or otherwise link information that is not maintained in a manner that would be considered personal information and should not be required to collect or store more information in order to comply with the exception in the proposal.

Section 11 (c), (d), and (e) include exemptions for certain data relating to the federal Health Insurance Portability and Accountability Act (HIPAA), the Gramm Leach Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA). The current language places companies in the untenable position of trying to parse through data to determine what information they have that is exempt and what is not. Imagine combing file by file through your business records to determine whether each individual piece of information is subject to, or exempt from, this law. Instead, the exemption should cover entities compliant with the federal acts.

The sections pertaining access, deletion and correction requests should have reasonable parameters. For example, in Section 2 given the time and expense related to compiling the information, the right to receive a report relative to the information being maintained should be limited to once a year, not twice a year as written.

And the obligation to respond to a request for, or for deletion of, information should be feasible and take into account available technology and the cost of implementation.

Section 9(2) requires businesses to act on a consumer's request within 45 days. This is an overly burdensome restriction of time and we would suggest at least a 60-day window for action with additional time for reasonably necessary extensions based upon the complexity of the request. This section should also be clarified to specify that the timeframe is based upon business days.

The private right of action in Section 12 is excessive and punitive and serves only to enrich the plaintiff's bar. The provision does nothing to enhance the goals of the proposed legislation. The proposed law provides ample regulatory and enforcement powers and significant penalties. The private right of action provision should be removed. The Connecticut breach notification statute (CGA Ann State Section 36a-701b) is one of the most challenging breach notification laws to administer. Laws in many other states include good faith exemptions and a potential risk of harm analysis prior to requiring notice. Other states also provide for supplementary requirements that must be satisfied for a private claim or class action to be pursued. The Act both permits a private cause of action and authorizes the Attorney General to bring a public enforcement action in connection with security breaches. It also allows for a broader, undefined penalty of whatever relief a Court determines as appropriate. Under the bill as currently written, businesses are vulnerable to potentially significant liability as a result the new remedies and private right of action provided in connection with certain breaches of security.

Relatedly, section 12(c) with the potential to cure is confusing. Is giving people notice an appropriate cure? Under the current Connecticut breach statute companies provide two years of identity protection. Will that be considered an appropriate "cure" to avoid additional liability? A specific safe harbor provision that comports with current law would be required if this proposal moves forward.

Because of the complexity and implementation burdens placed on Connecticut businesses under this proposal, the effective date of January 1, 2020 should be extended at least to July 2021. Because of the sweeping nature of this law and its complexity and cost, a two-year, or more, implementation period is eminently reasonable.

As indicated above, the Act imposes significant new requirements on businesses regarding how and when they must respond to consumers' requests for information relating to their personal information that is collected, sold or shared with third parties. The record-keeping obligations associated these new requirements could potentially be extensive, given the anticipated volume of consumer requests. For companies with subsidiaries and affiliates, computer systems coordination and compatibility may be a challenge. Establishing the procedures for consumer access to their personal information, along with the training of personnel to handle and comply with these requests, will be significant. These are among the reasons why the bill should have a delayed effective date.

As we mentioned at the outset, Connecticut already has in place comprehensive state insurance laws and regulations governing the confidentiality of personal information. The *Connecticut Insurance Information and Privacy Protection Act (CT Gen. State. Ann Sec. 36a-975); the Privacy of Consumer Financial Information (CT ADC Se. 38a-8-105); and the Safeguarding of Customer Financial Information (CT ADC Sec. 38a-8-124)* regulate the collection, use and disclosure of information gathered in connection with life and health policies, contracts or certificates of insurance issued or delivered in Connecticut. These requirements govern the treatment of nonpublic personal health information and nonpublic personal financial information about individuals by all licensees of the Department of Insurance and are intended to afford individuals privacy protections that supplement those provided at the federal level in the Gramm-Leach-Bliley Financial Modernization Act (GLBA), Pub. L. 106-102, 113 Stat. 1338, 1415-17 (1999) (codified at 15 U.S.C.A. Section 6716). Existing requirements must be taken into consideration by policymakers considering sweeping new requirements.

In conclusion, we respectfully encourage the Committee to give further thought to the far-reaching implications of any new legislation before superimposing another layer of redundant or conflicting regulatory requirements on those already in place.

We thank you for your consideration of our comments. Please contact John Larkin at (860) 508-9924 with any questions.