July 28, 2023

Chair Katie Johnson
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO  64106
Via email to LAlexander@naic.org

RE: Comments regarding July 2023 Draft of Consumer Privacy Protection Model Law (#674)

Dear Chair Johnson,

The American Property and Casualty Insurance Association (APCIA) appreciates the opportunity to provide initial comments in response to the updated draft of Consumer Privacy Protection Model Law #674.

APCIA is the primary national trade association for home, auto, and business insurers. APCIA promotes and protects the viability of private competition for the benefit of consumers and insurers, with a legacy dating back 150 years. APCIA members represent all sizes, structures, and regions—protecting families, communities, and businesses in the U.S. and across the globe.

We appreciate the opportunity to share APCIA’s initial thoughts on this updated draft. Our members are very invested and engaged in this process, as demonstrated by our participation in open calls, national meetings, and the interim meeting, as well as our submission of written feedback at various points throughout the process. We recognize there are incremental improvements in this draft, for example eliminating prior consent requirements for cross-border data sharing. Nevertheless, significant concerns remain with the workability of many of the current draft’s requirements.

We have also included a redline with specific language recommendations and will share additional feedback as this process evolves and our members more thoroughly review the text and its potential impacts. We also note that our previous feedback remains unaddressed, and welcome understanding the Working Group’s reasoning so that we may clarify our concerns or offer modified recommendations.

During the Working Group’s July 25th conference call, it was noted that regulators knew this current exposure draft would change and that, in fact, a redline version 1.3 is expected to be exposed in a couple of weeks. Understandably, this is concerning to our members that have devoted considerable time to analyze and suggest drafting language for Version 1.2. An effective collaborative process requires regulators and interested parties to all collaborate from the same document with meaningful time for review.

These issues are complex and we must recognize the necessary interplay with existing state and federal legal obligations as well as cross-sectional alignment within the model itself. As such, it is critical that the remainder of this process not be rushed. Rushing could result in unintended consequences and a Model that cannot be adopted uniformly, if at all. Ultimately, this will only compound the emerging patchwork of inconsistent state privacy laws rather than ameliorate it.
The following significant concerns are intended to be helpful and show that the draft Model has a long way to go before being finalized.

**Definitions**

Our members noted several changes to definitions in this new draft. We have provided initial feedback on some of those changes here, but our members have not had sufficient time to review those changes in detail. We would request that the Working Group consider focusing one of the upcoming open calls on further discussion of this topic, as the definitions and how they are applied will be critical to how we understand and respond to other provisions of the draft. We have included more thorough revisions in our redline, but a few of the definitions that we recommend changes to or require clarification for include:

**“Additional Activities”**
- Although the category of “Additional Permitted Transactions” has been removed, there are repeated and significant references to “additional activities” throughout the updated draft. We recommend that this term be defined clearly, and clearly distinguished from the what activities are considered an “insurance transaction”, also making sure to address any gaps.

**“Biometric Information”**
- This should be aligned with the Virginia or California definition, which we have previously provided.
- Additionally, “sleep, health or exercise data” should not be included in this definition.
- We request it be made clear that neither photographs nor videos are biometric information.

**“Consumer”**
- Under this definition, a consumer is someone who has engaged in an insurance transaction. That seems to start at quote or application. That will imply that if someone accesses the website, there are no limits to data collection and use, but once the quote process starts, then they are considered a consumer and all rules apply.
- Also- would a worker’s compensation claimant be considered a consumer? We recommend reverting to language in NAIC Model Reg 672-1, which stated that a worker’s compensation claimant was not a consumer if the insurer provided privacy notices to the worker’s compensation policyholder and the insurer did not disclose nonpublic personal information other than as permitted under the regulation. We would also seek clarification on whether a group insurance member would be considered a consumer.

**“De identified”**
- California and Virginia already define de-identified information. For consistency’s sake and to ease compliance, we urge the Working Group to pick one of those definitions rather than creating yet another one.

**“Insurance Transaction”**
- We have several outstanding concerns with this definition, which are provided in redline. A few primary points are included below.
- We recommend clarifying that a quote is considered an insurance transaction.
- We recommend the deletion of the language “any mathematical-based decision that involves a consumer’s personal information.” As we have raised previously, this language is unclear and confusing and should either be clarified or deleted.
“Nonaffiliated Third Party”
• It should be clarified that a third-party service provider is not an unaffiliated third party.

“Personal Information”
• We suggest considering deleting all sub-provisions. This would then better mirror the definition of personal data in all other laws.
• It should be clarified that publicly-available information is not personal information, in alignment with the approach taken generally by other comprehensive privacy laws.

Third Party Oversight
Although some improvements have been made in this section, the provisions regarding requirements for oversight of third-party service providers remain overly broad and prescriptive. The updated draft includes a number of requirements that it is unrealistic to expect vendors will agree to. One example is the requirement that a third-party service provider is required to comply with each individual licensee’s privacy practices. This is not workable in practice, since a vendor cannot reasonably comply with thousands of companies’ privacy practices. Contractually requiring data usage to be limited to the contractual purpose and compliance with applicable laws should be sufficient. Licensees are also not able to prevent vendors from having subcontractors. The typical limitations for these types of issues are that the vendor can only use the information as provided for in the contract and cannot sell it, which would be a workable alternative.

Our members also note concerns with the implications of including publicly-available information in these requirements, and in other places throughout the draft. It is unclear in this section specifically why a provision related to publicly available information is necessary and, even if so, why is it limited to claims. We recommend not applying the requirements of Section 3(C) to publicly available information. APCIA also recommends aligning Section (3)(F) with the provisions regarding re-use and re-disclosure included in Model 672, which our members believe addresses those topics thoughtfully and effectively. We also recommend several other edits included in-text in our accompanying redline.

Data Minimization
APCIA is glad to see that the earlier provision requiring consent for overseas data sharing has been removed. This constitutes a significant and critical improvement to the data minimization section and the draft as a whole. Regarding Section 4(B), such data usage is a common topic in state breach disclosure laws. Several such laws include a thoughtful good faith exemption, explicitly defining it as “not-a-breach” if the insider who sees something they should not makes no inappropriate use of the data. We recommend including such language.

Sharing Limitations
APCIA members found this section to be one of the most problematic in terms of remaining issues. First, the provisions included in Section 5 are broader in scope than sharing, as they specifically also address “processing, collection, and retention” as well. We request this section be limited to sharing specifically for additional clarity. Our members are particularly concerned by the requirements outlined in Section 5(A)(8). We note that no other law includes the requirements stated in Section 5(A)(8)(a) and (b). As a general practice, companies are permitted to transfer data without qualification. In particular regarding Section 5(A)(8)(b), during due diligence, a recipient may need to share the information with the recipient’s counsel or other experts. Under this provision, it is not clear if that is even feasible. For these many reasons, APCIA requests these provisions be stricken.
Our members have also raised concerns that the implications of this language for joint marketing do not match the stated intent towards the joint marketing issue that was included in the cover letter. Specifically, Section 5(A)(14) will require edits to more clearly enable joint marketing between financial institutions as authorized by the Gramm-Leach-Bliley Act (GLBA) and subject to the Working Group’s intended opt-out requirement. Regarding Section 5(A)(15), marketing of an insurer’s own products should be considered an insurance transaction. Also, it is unclear how insurers are expected to provide consumers with an opportunity to opt-out if they haven’t interacted yet. Finally, requiring written consent is inconsistent with the notion of an “opt-out” and in effect changes this to an “opt-in” standard. For these reasons, and others, we request Section 5(A)(15) be removed.

Section 5(B) imposes an unreasonable requirement regarding sharing with nonaffiliated third-parties. This requirement may not be feasible, as insurers need to share this information with third party service providers to administer claims and for other insurance purposes. Our members recommend perhaps applying this requirement only to “additional activities”, or explicitly allowing such sharing for the purposes of “insurance transactions”.

Finally, Section 5(A)(9) suggests that information may be shared with an affiliate only for auditing purposes. Current law allows personal information to be shared amongst affiliated entities, which is necessary to the operation of insurance holding company systems. There are other legitimate reasons to allow sharing with affiliates to conduct usual and customer insurance and related transactions.

**Consumers’ Consent**

Regarding consumers’ consent, our members had several recommended changes to these provisions. First, it is critical that this section has a clear exception for detecting or preventing fraud. The language in Section 5(A)(6) would work well and could be replicated here. The language of this section also does not currently make clear that consent may be provided electronically. We recommend including clarifying language that allows consumers to provide consent electronically or verbally, in addition to in writing.

In addition, APCIA strongly recommends that Section 6(B) be updated to align with the relevant provision from either the Virginia or California privacy law. Our members also have concerns with the amount of detail required for consent. That level of detail will require a long form that will not be digestible and will undermine efforts towards clarity. For example, listing all the underwriting companies isn’t entirely helpful when they think of the company as its commonly-known, primary-brand name. Most existing privacy laws focus more on explaining the purpose and use of the data, rather than these additional factors for consent. We recommend that approach. If this section is largely retained, we recommend at minimum combining Sections 6(B) and 6(C) into one consolidated set of requirements and process for consent for additional clarity.

**Retention and Deletion**

APCIA has significant concerns with this area, which is in our members’ view currently one of the most unworkable parts of this draft. Our primary issue concerns Section 7(B), which requires a licensee to review all of a consumer’s personal information in its possession, in addition to its retention schedule, and to determine whether the reasons for collecting or processing that information remain. This is a completely unworkable requirement. It is not feasible for a company to review all consumer personal information in its possession on an annual basis. This provision also suggests some misunderstanding about how insurers’ retention schedules work. They are not based on a person, but rather, are based upon categories of business records. For example, claims business records are retained for a certain number of years from the data the claim is closed. A consumer’s claim information may be retained for a longer or shorter period of time than their policy information. For those reasons, all of a consumer’s data will not be ready to be
deleted on the same day or even necessarily in the same year. A company can review the retention schedule annually to determine if it is compliant with existing laws, which is a much more reasonable alternative.

In terms of other issues, Section 7(A)(2) should be broadened to compliance with any legal obligation, not only those involving certain types of transactions. Insurers are required to meet all of their legal obligations and the language of this draft should not prevent them from doing so. Section 7(C) also seems to rely on the idea that insurers are making constant individualized determinations, which is not how these processes work in practice. It is a positive change that this draft recognizes that some systems will not allow for deletion or deidentification. However, several subsections of this provision still seem to have a disconnect from some of the operational realities of insurers’ business models and the limitations of legacy systems. We have further elaborated on these areas in our redline and recommend language changes to address those concerns. In Section 7(C)(3), there is also an unrealistic time frame required for transitions from legacy systems. APCIA suggests including language to make this more adaptable as is appropriate. Finally, Section 7(C)(4) imposes an impractical and unrealistic requirement for third-party providers. First, many contracts with third-party providers explicitly require those providers to preserve data beyond the contract termination date in order to comply with legal retention obligations. As worded, this clause in the Model Act would have the effect of voiding those survivorship clauses. Second, third-party providers have the same practical limitations to deletion as insurers do. Data is interlinked, backed up and handled in complex ways that cannot be simply undone on the very same day as a contract ends. This is especially true if contract termination is unscheduled.

Finally, third-party service providers may have independent relationships with the consumer (e.g., car rental companies, banks, body shops, etc.) and may not be able to follow insurance industry practices or these rules without undue hardship. This will greatly reduce the service providers available for use by insurers.

As such, we recommend this provision be truncated to note that third party service providers shall delete such information as soon as is reasonably practicable. For that same reason, we also recommend that Section 7 exclude data stored in backups.

**Notices and Delivery of Notices**

There are several areas APCIA would like to highlight regarding the requirements for both content and delivery of notices.

Section 8(B)(1) impacts joint marketing. This provision could require an insurer to send privacy notices as soon as the licensee receives a consumer’s information from a joint marketing partner financial institution. That sharing is covered by the other financial institution’s privacy policy and notice already send to the consumer. The notice may be required even if the insurer never markets or shares the consumer’s information, which would likely cause consumer confusion. We request the language be updated to better reflect the intent expressed in the cover letter to permit joint marketing agreements. Our members also noted an additional practical concern with this requirement. The provision states that the initial notice must be given when the insurer first collects the personal information. In order to give the initial notice, a licensee can rely on having a privacy notice on the website, but the consumer has to agree to accept notices electronically under the UETA before the electronic privacy notice is delivered. This constitutes a practical problem. Once again, we recommend reworking this provision if it is retained.

In addition, the requirements of Section 8(C) and (E) should include a materiality trigger. This seems more consistent with the intent expressed in the cover letter and throughout the rest of the draft. Regarding
Section 8(C)(2), it is not feasible for licensees to provide a privacy notice to third-party claimants and beneficiaries, for a number of reasons. Insurers may not have sufficient contact information for these individuals, and in many cases, beneficiaries are not aware that they are a beneficiary. This means a licensee may have to explain its relationship to them, as the individual will not know. This is unnecessary and would cause confusion. We recommend removing this provision.

We would like to raise again a concern with the language of Section 9 that was mentioned in the interim meeting, as well as in earlier comments. The language around notices in Section 9 refers to a “list of persons” as opposed to “categories of” sources or third-party service providers. APCIA reiterates our position recommending that this language refer to categories rather than a list of individual persons. It is not only likely infeasible, but also a security risk to share a list of specific persons and third parties with whom a consumer’s information was shared. This could also create confidentiality concerns.

We recommend the provision Section 9(A)(7)(b) be limited to apply only to sensitive personal information. Regarding 9(A)(10), it will not be feasible to adequately explain the complexities of complex insurance retention policies in this context, especially given the extensive and worsening patchwork of legislative and regulatory requirements insurers are subject to. This requirement also has the unintended consequence of undermining the requirement that notices be clear. We suggest a more reasonable alternative in our redline language. Regarding Section 10 on the whole, it seems unnecessary to create a separate privacy notice that must be sent to consumers annually when the notice addressed in Sections 8 and 9 is not required annually unless there are material changes. For this reason, we recommend consolidating all of this information into one notice, to be provided on the same schedule as the notice referenced in Sections 8 and 9.

Section 11, regarding delivery of notices, also has a number of outstanding issues. In present form, it does not address what happens when a consumer is interacting via telephone. In addition, this section only makes sense if the only “consumers” are insureds, but would make little or no sense in the context of claimants, witnesses, commercial-insured employees, etc. As mentioned in our feedback on the definitions, further clarification on who is a “consumer” under this Act is necessary for this to work. Our members also recommend combining Sections 11(C) and (D) into one clear, consolidated provision. 11(D) is more clearly written, so we recommend merging 11(C) into 11(D), making the language of 11(C) exceptions in the new combined provision.

APCIA would like to reiterate our members’ concern regarding the requirements for delivery receipts, which we raised in our comments on the initial draft, on an open call and in the interim meeting in Kansas City. No other privacy law or industry requires proof of receipt for notices and the expectation that consumers would provide such a receipt electronically or otherwise. Moreover, as we raised in our previous comment letter, many email systems do not return read receipts, and users can turn off the sending of read or sent receipts. It is also unclear how a consumer would acknowledge receipt of viewing the notice on the website. In addition, no equivalent ‘proof of receipt’ is required for paper delivery and we do not see a clear reason to require a higher standard for electronic delivery. The requirement for delivery receipts is both unnecessary and infeasible, and we continue to recommend it be removed.

Access to Personal and Publicly Available Information
Section 12(A) should be narrowed to a more appropriate scope. It is feasible to make a request for data that the third party has under a contract with licensee, not just all of the data that the third party has about a given consumer. Our members also oppose the inclusion of publicly available information in this section. Including publicly available information here would require disclosing every piece of information an insurer possesses about a consumer, whether or not the insurer relies upon that information. This is unnecessary,
Insurers are already required to explain adverse underwriting decisions and claim denials. For these reasons, we suggest moving this provision to Section 14 (if that Section is retained) and allowing consumers to see “publicly available information” if it was used in reaching an adverse underwriting decision. Additionally, it is unclear what Section 12(E) is intended to address. These requirements should be limited to consumers.

Although the time frames in Section 12(B) are improved, they are still not uniform with California. We would recommend fully aligning them with what is required in CPRA, which references “calendar days” rather than business days, and includes language to allow for an additional 90 days if needed.

**Correction of Personal and Publicly Available Information**

Our members have various concerns with the obligations imposed and approach taken regarding correction. The obligation that licensees and their third-party service providers correct publicly available information is problematic. Despite the efforts in Section 13 to detail a refusal process, this obligation puts licensees in the inappropriate position of disputing information prescribed in government records with consumers.

We recommend an alternate approach to addressing publicly available information- to reference a licensee’s obligation to correct internal records once the relevant government office has amended the consumers’ information. It should be the consumers’ obligation to provide licensees supporting documentation from the government office to evidence this change. Additionally, some data must be verified before insurers can make a change, and some changes will affect the premium and require complete recalculations, possibly even re-underwriting of the policy. Those processes take time and 15 days is completely unworkable from that perspective.

The timeframe in this section should mirror the timeframe for access in Section 12. We emphasize that these time periods are even more unrealistic if the requirement to correct publicly available information is retained. We recommend the changes suggested for the timelines in Section 12 above also be applied here.

Section 13(B)(2)(b), requiring a specific legal basis to not correct information, is also problematic. Our members would like to know if accuracy would be considered a legal basis in this context. We note that the CPRA regulations provided details around correction that could be utilized as a template to clarify this Section and help harmonize requirements. In general, we believe more flexibility is necessary. The remedies suggested in 13(D) and (E) are more appropriate to strike the right balance.

As a best practice, consumers should start the correction where the actual bad data originated. Then, following the procedure outlined, they should pass it downstream to the licensee. This is a more effective, efficient and appropriate system.

**Adverse Underwriting Decisions**

Although Model 670 includes provisions related to Adverse Underwriting Decisions, APCIA recommends this content not be included in this updated Model. Currently, there are other state laws that govern this area effectively. This was likely not have been the case when Model 670 was drafted, which would explain the topic’s inclusion here at that time. Since the legislative landscape has developed to more appropriately address this in other places, this content no longer belongs in the privacy Model. We recommend removing this section from the Draft. Should this Section be retained, however, APCIA has included several in-line language suggestions in redline to improve its workability.
Sections 16-20
APCIA previously submitted comments on these Sections for consideration. We would request that those comments still be considered with respect to the new Draft.

Sections 33
We believe that a transition and delayed enforcement period will be necessary. Our members request three years minimum to implement these provisions, and potentially will need longer for the provisions regarding third-party service providers.

Conclusion
APCIA thanks the Working Group for its hard work and continued engagement on this project. We remain committed to providing constructive feedback and respectfully urge the Working Group to not rush this process.

We welcome the opportunity to discuss these concerns and recommendations with the Working Group.

Sincerely,

Shelby Schoensee
Director, Cyber & Counsel