COMPILATION OF WRITTEN COMMENTS ON THE PLAN FORWARD FOR THE PRIVACY PROTECTIONS (H) WORKING GROUP
MAY 31, 2024

In order to begin that important work, we first need to determine a path for the working group to proceed in order to accomplish our charges.

We are seeking comments in two areas:

1. **Does the working group want to continue work on Draft NAIC Privacy Model #674?**
2. **Or Revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?**

Summary: 20 responses - 10 states (MN, AK, NE, ME, IA, RI, SD, CA, MO; ND); 9 industry; 1 consumer representative
11 PDFs attached
Continue #674: CA, MO
Revise Existing: MN, AK, NE, IA, RI, SD, ND
Could Support Either: ME, Privacy4Cars, consumer representative
Suggested Different Approach: Nonprofits Insurance Alliance

Received from MN 5/17/24:

Supports revising existing model – see PDF

Hi Lois,

While I believe the working group could come to similar outcomes via either path, Minnesota votes to revise Model #672 (and #670, if necessary) instead of continuing with Model #674.

Thanks,

T.J. Patton

Received from AK 5/28/24:

Supports revising existing model – see PDF

I know that a lot of time and effort went into the drafting of Model #674, from both regulators and industry commentors. Draft 674 had the intent of bringing both acts 670 and 672 to modernized regulation. The feedback received was very valuable in trying to get it workable for industry and regulators. Continued work on the exposed June 2023 Model #674 might be helpful to the working group to keep from going backwards and adding more time to a rapidly changing and vulnerable area in insurance regulation.

However, I do also understand that having a good number of new members to the working group means new eyes and perspectives and going back to the beginning to revise Models #670-672 may be easier overall plus incorporating the industry draft provided.

Chelsy Maller

COMPILATION OF WRITTEN COMMENTS ON THE PLAN FORWARD FOR THE PRIVACY PROTECTIONS (H) WORKING GROUP
MAY 31, 2024

In order to begin that important work, we first need to determine a path for the working group to proceed in order to accomplish our charges.

We are seeking comments in two areas:

1. **Does the working group want to continue work on Draft NAIC Privacy Model #674?**
2. **Or Revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?**

Received from McIntyre & Lemon, PLLC 5/29/24:

Supports revising existing model – see PDF

Thx. We will do at ABA. Considering joining an industry letter as alternative

Jeffrey M. Klein, Esq.

Received from NE 5/29/24:

Supports revising existing model – see PDF

We would prefer to work with the industry submission

Martin Swanson

Received from Lemonade 5/29/24:

Supports revising existing model – see PDF

Prefer revising the existing models taking into account the draft submitted by industry.
Thank you.

Scott Fischer

Received from Privacy4Cars 5/29/24:

Supports either if compliance is enforced – see PDF

Dear Lois,

COMPILATION OF WRITTEN COMMENTS ON THE PLAN FORWARD FOR THE PRIVACY PROTECTIONS (H) WORKING GROUP
MAY 31, 2024

In order to begin that important work, we first need to determine a path for the working group to proceed in order to accomplish our charges.

We are seeking comments in two areas:

1. **Does the working group want to continue work on Draft NAIC Privacy Model #674?**
2. **Or Revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?**

Please find attached Privacy4Cars's Response to the NAIC's Request for Written Comments on the Path Forward for the Privacy Protections (H) Working Group's consideration in their decision.

Should you require any further information, please do not hesitate to contact us.

Kind regards,
Liz

Elizabeth Magana

Received from ME 5/30/24:

Could Support Either

Good Morning Lois,

The following are the comments from Maine:

- The actual platform being revised doesn't matter as much as the substantive issues. It's unclear what Industry specifically objected to about 670 and 674, and without that knowledge, it's difficult to advocate for one platform over the other. Having said that, the additions made by the Industry draft appear to flesh out much of those issues, so it might be easier to work from that.
- As to the substantive issues:
    - We dislike making the HIPAA exception jurisdictional – it appears to be saying they're deemed to be compliant with state law whether or not they actually comply with any law at all.
    - We'd like some clarity on adverse action notices, is this a particular point of friction?
    - What are the specifics of the GLBA exception, is it entity-level?

Apologies for raising more questions than comments, I think once we pick a draft and move forward with it, the task will be easier.

Stacy L. Bergendahl

Received from Nonprofits Insurance Alliance 5/30/24:

COMPILATION OF WRITTEN COMMENTS ON THE PLAN FORWARD FOR THE PRIVACY PROTECTIONS (H) WORKING GROUP
MAY 31, 2024

In order to begin that important work, we first need to determine a path for the working group to proceed in order to accomplish our charges.

We are seeking comments in two areas:

1. **Does the working group want to continue work on Draft NAIC Privacy Model #674?**
2. **Or Revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?**

Suggested using differential privacy and homomorphic encryption – see PDF

Christopher Reed

Received from IA 5/30/24:

Supports revising existing model – see PDF

Jordan Esbrook

Received from RI 5/30/24:

Supports revising existing model – see PDF

Lois:

Good Morning! Rhode Island would recommend following Path #2 - Revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration.

Let me know if you have any questions. And Have a Good Afternoon!

Patrick Smock

Received from The Committee of Annuity Insurers 5/30/24:

Supports revising existing model – see PDF

Hi Lois,

I hope all is well.

On behalf of the Committee of Annuity Insurers, please find our comments attached on the path forward for the PPWG.

Please let me know if you have any questions or any trouble with the file.

COMPILATION OF WRITTEN COMMENTS ON THE PLAN FORWARD FOR THE PRIVACY PROTECTIONS (H) WORKING GROUP
MAY 31, 2024

In order to begin that important work, we first need to determine a path for the working group to proceed in order to accomplish our charges.

We are seeking comments in two areas:

1. **Does the working group want to continue work on Draft NAIC Privacy Model #674?**
2. **Or Revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?**

Best,

Al

Alexander F. L. Sand, Eversheds Sutherland

Received from Healthcare Consumer Advocate 5/30/24:

Could Support Either – see PDF

Hi Lois,

Attached are my comments.

Harry

Harry Ting, NAIC Consumer Representative

Received from SD 5/30/24:

Supports revising existing model – see PDF

Hi, Lois,

South Dakota has voiced concerns with draft Model #674 and submits these comments. Model #674 carries the residue of Model #670, adopted by a minority of states, and a blend of single-state privacy law enactments. These inclusions will likely hinder uniform adoption. We should set aside Model #674 and create a solid, sensible national standard that is capable of uniform enactment. We should protect consumers and listen to industry concerns during drafting, working in an open forum. Model #672 was universally adopted by the states and establishes basic privacy protections that can be enhanced and modified; it is a logical foundation for this work. Finally, with more states passing industry agnostic privacy laws each year, the likelihood of successfully implementing a uniform insurance privacy model diminishes. We need to set a course soon and get drafting.

Thanks,

Frank A. Marnell

COMPILATION OF WRITTEN COMMENTS ON THE PLAN FORWARD FOR THE PRIVACY PROTECTIONS (H) WORKING GROUP
MAY 31, 2024

In order to begin that important work, we first need to determine a path for the working group to proceed in order to accomplish our charges.

We are seeking comments in two areas:

1. **Does the working group want to continue work on Draft NAIC Privacy Model #674?**
2. **Or Revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?**

Received from Joint Trades 5/30/24:

Supports revising existing model – see PDF

Lois,

Good afternoon. Please find attached a joint trade comment letter in response to the Privacy Protections Working Group's request for feedback on the appropriate path forward for the working group to accomplish your charges "to draft a new/revised Privacy Protections Model Act to replace/update NAIC models such as Model #670 and/or Model #672."

We appreciate this opportunity to share our thoughts and look forward to continued conversations around this important topic. Please do not hesitate to reach out if you have any questions.

Many thanks,

Kristin Abbott, APCIA

Received from ISO 5/30/24:

Supports revising existing model – see PDF

Hello Lois,

Attached please find ISO's comments on the path forward for the privacy protections working group. Please let us know if you have any questions.

Nancy Crespo

Received from the Coalition of Health Insurers 5/30/24:

Supports revising existing model – see PDF

COMPILATION OF WRITTEN COMMENTS ON THE PLAN FORWARD FOR THE PRIVACY PROTECTIONS (H) WORKING GROUP
MAY 31, 2024

In order to begin that important work, we first need to determine a path for the working group to proceed in order to accomplish our charges.

We are seeking comments in two areas:

1. **Does the working group want to continue work on Draft NAIC Privacy Model #674?**
2. **Or Revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?**

Attached is comment letter from the Coalition of Health Insurers. Please give me a call if you have any questions. Thank you.

Chris Petersen, Arbor Stategies, LLC

Received from National Association of Professional Insurance Agents 5/30/24:

Supports revising existing model – see PDF

Good afternoon. Please find attached the comments of the National Association of Professional Insurance Agents in response to the Chair's request for feedback on the path forward of the Privacy Protections (H) Working Group. As always, we appreciate the opportunity to provide the independent agent perspective on the Working Group's important charges and look forward to speaking further about these important issues during the Working Group's upcoming calls.

Please do not hesitate to reach out to me if I can be of assistance in any way in advance of the Working Group's next call.

All the best,
Lauren

Lauren G. Pachman, PIA

Received from CA 5/30/24:

Supports Continuing #674 – see PDF

Good evening, Commissioner Beard-
Attached, please find California's submission in response to your request for comment on PPWG direction. Please let me know if you have any questions.

Additionally, I wanted to point out a few minor issues with the privacy laws comparison chart, which NAIC staff kindly prepared. Speaking generally, these models define and use key terms in very different ways (which I point out in the attached letter); consequently it is very hard to do a straight 1:1 comparison of their scope and effect.

The chart has a few inaccuracies:

COMPILATION OF WRITTEN COMMENTS ON THE PLAN FORWARD FOR THE PRIVACY PROTECTIONS (H) WORKING GROUP
MAY 31, 2024

In order to begin that important work, we first need to determine a path for the working group to proceed in order to accomplish our charges.

We are seeking comments in two areas:

1. **Does the working group want to continue work on Draft NAIC Privacy Model #674?**
2. **Or Revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?**

-Model 670 does provide a private right of action (See Section 20 "Individual Remedies"); this isn't reflected in the chart.
-Model 670 provides a right to opt-out of disclosures for marketing (i.e.: opt-out of certain processing) (See Section 13(k)); also not reflected "Consumer Rights" or "Business Obligations" portions of the chart.
-In addition to certain opt-out rights shown on the chart, Model 674 adopts an opt-in standard for marketing use of "sensitive personal information" (See Section 5(F)), and an opt-in standard for non-insurance uses of personal information (See Section 5(G)) (Note that marketing of insurance products and joint-marketing activities are considered insurance uses and not subject to the opt-in standard)
-Rather than opt-out, Model 674 prohibits sale of personal information (See Section 5(H)). So far, no stakeholder has commented that they sell consumer data, so this provision should be uncontroversial.
-Model 670 does regulate third-party service provider arrangements; however, these are defined as "insurance support organizations" in 670. Functionally, there is little difference between ISOs in 670 and TPSPs as defined in other statutes.

Thanks for your consideration. Looking forward to discussing these important issues with the Working Group.

-DD

Received from MO 5/30/24:

Supports Continuing #674 – see PDF

Hello – attached are my comments. I think we need to move forward with Model #674. Thanks,
CMA

Cindy Amann

Received from ND 5/31/24:

Supports revising existing model – see PDF

Hi Lois,

COMPILATION OF WRITTEN COMMENTS ON THE PLAN FORWARD FOR THE PRIVACY PROTECTIONS (H) WORKING GROUP
MAY 31, 2024

In order to begin that important work, we first need to determine a path for the working group to proceed in order to accomplish our charges.

We are seeking comments in two areas:

1. **Does the working group want to continue work on Draft NAIC Privacy Model #674?**
2. **Or Revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?**

I hope you are well! I apologize about the delay.

As for option 1 or 2 specifically, North Dakota would vote for option 2 at this time. We look forward to continuing discussions.

Thank you.

Santana

STATE OF CALIFORNIA
Ricardo Lara, Insurance Commissioner

DEPARTMENT OF INSURANCE
Legal Division, Government Law Bureau
300 Capitol Mall, 17th Floor
Sacramento, CA 95814

Damon Diederich
Privacy Officer / Attorney IV
TEL: 916-492-3567
FAX: 916-324-1883
E-Mail: Damon.Diederich@insurance.ca.gov
www.insurance.ca.gov

May 30, 2024

VIA ELECTRONIC MAIL

Commissioner Amy L. Beard
Indiana Department of Insurance
311 West Washington Street
Suite 300
Indianapolis, IN 46204-2287
[E-mail address withheld for privacy]

SUBJECT: NAIC Privacy Protections Working Group –
Request for Comment re: Working Group Direction and Approach

Dear Commissioner Beard:

Thank you for agreeing to take charge of the Privacy Protections Working Group. The Working Group is at a crossroads, and you've sought input as to which direction it should pursue. I strongly encourage the Working Group to continue development of Model #674. Continuing development of Model #674 ensures that NAIC will keep pace with contemporary privacy regulation and provide strong protections for consumers. Departing from development of Model #674 will mean discarding years of work.

Developing a new model based on Model 672 will result in flawed, inadequate privacy protections, or will require investment of significant time to bring the model up to modern privacy standards. Developing a cohesive statutory scheme requires consistent use of defined terms, and careful review for meaning and syntax; this process takes investment of time. Simply engrafting concepts from Model #674 onto #672, as industry have proposed, represents only a small part of the work needed to create an effective privacy law.

GLBA / Model 672 is an outlier among privacy laws. In the two decades since GLBA was adopted, most of the world's leading economies, many growing economies, and many states of the United States, have adopted privacy laws. The majority of these laws have followed the effective consumer protection framework contained in the European General Data Protection Regulation. Other than adoptions of Model 672, no privacy law developed after GLBA has followed the GLBA approach. States widely adopted Model 672 because GLBA would preempt

state regulation of insurance privacy, if the states did not enact Model 672. Lacking basic privacy rights like access, correction, and consumer data choice, Model #672 doesn't even allow consumers to opt-out of third-party data sharing for joint marketing. This violates basic ideas of privacy rights and makes no sense, given that consumers can opt-out of affiliate marketing under FCRA. Model #672 has little to recommend itself, other than low compliance costs for insurers.

There is new impetus to enact strong privacy protections: the recent Change Healthcare breach may be one of the most significant breach events ever. This event may overcome the inertia which has hindered prior attempts at Federal legislation, making it important that state insurance regulators act quickly and decisively to ensure robust privacy protection for insurance consumers.

Privacy lies at the heart of almost every major issue currently before NAIC. Insurance businesses are using telematic and electronic means to collect more information about consumers than ever before, are pooling that data into vast "data lakes," and are using that data to train Artificially Intelligent and Machine Learning ("AI/ML") systems. These data tools are being used to develop new marketing practices, offer new coverages, and engineer new underwriting models, including AI/ML-based underwriting where coverage decisions may be made without any human input. Moreover, adverse conditions in some market segments, such as homeowners' insurance, may encourage insurance businesses to move into non-insurance spaces to bolster profitability (for example, pet wellness, as reflected in Model #633), leading to potential regulatory gaps. And, whether we like it or not, organized, institutionalized hacking is now a reality; these groups specifically target data-rich entities like insurance businesses.

Insurance has always been a data-intensive industry, but legacy privacy laws like the Fair Credit Reporting Act ("FCRA") / Model #670 and the Gramm-Leach-Bliley Act ("GLBA") / Model #672 simply are not designed to provide meaningful privacy protection in light of modern trends. These laws are decades old (four decades in the case of Model #670, and two decades in the case of Model #672); their drafters could not have anticipated the fluidity with which personal information is currently collected, the many new purposes for which personal information is processed and exchanged, or the scale and speed at which these transactions are taking place.

Not only do Models #670 and 672 fail to adequately address technological developments since their adoption, but they contained flaws at the time of their adoption. Both #670 and #672 are limited in scope to recipients of insurance products for "personal, family, or household purposes." They offer no protection to broad classes of individuals whose personal information is used in connection with commercial coverages, such as workers' compensation or fleet motor vehicle coverages. People whose personal information is provided to insurers in connection with those commercial coverages have no choice about which insurer is selected by their employer and no privacy protections with respect to their personal information. As discussed above, GLBA / Model #672 lacks even the basic rights of access, correction, and choice for any consumer; these are staples of every privacy law enacted since FCRA. For a comprehensive discussion of why Model #670 is a preferable basis for developing a privacy law, as compared to

Model #672, please see the March 3, 2022 letter to Katie Johnson, attached as Exhibit A to this letter.

The above example regarding regulatory gaps created by the "personal/family/household" distinction in existing privacy laws underscores how essential definitions are to determining the effectiveness of a statute. The definitions in Model #674 have been thoroughly reviewed and updated to prevent gaps in privacy protection. Restarting the drafting process from a different source (e.g.: Model #670 or 672) would require duplication of this painstaking work.

The complexities of modern data use need to be counterbalanced by robust consumer privacy protections. A modern insurance privacy law should:

- Protect consumers throughout all parts of the insurance data ecosystem and at all stages of the consumer's interaction with the licensee;
- Provide effective notices and transparency, including information about sources of personal information, uses of personal information, and disclosures of personal information;
- Inform consumers when personal information negatively impacts the price or availability of coverage for a consumer, and allow the consumer to verify or contest the underlying information;
- Permit the consumer to exercise meaningful choice about whether and how their personal information is used for purposes unrelated to the consumer's insurance coverage; and
- Provide data minimization and effective records retention requirements as a safeguard against institutionalized hacking.

Model #674 already contains all the essential consumer protections of a modern privacy law, which is why the Working Group should continue to focus on development of this Model. Continuing to receive stakeholder input on Model #674 (none has been received since July 2023), and revising the Model accordingly, is the best and most efficient way to develop an effective consumer privacy law.

In closing, I want to emphasize the big picture: privacy is about average, everyday people and how personal information significantly impacts their lives. As regulators, we should want consumers to be informed about how their data is being used and what their rights are; we should further want to ensure that data collection and use provides safeguards for that data, and is consistent with the reasonable expectations of the consumer.

Privacy is about preventing a person with a common name from being charged more, or denied coverage, because their data has become commingled with someone else. Helping a person leaving an abusive relationship be reassured that their former partner no longer has access to their information. Preventing the elderly from being victimized by targeted fraud arising from data breaches.

It's very easy for the privacy conversation to become abstract and mired in discussion of acronyms and terms like "customer vs. consumer," "opt-in vs. opt-out," "FAST Act notices," "legacy systems," "third-party service providers," etc. My hope is that our focus as a Working Group can remain on the consumer and how to help them navigate an increasingly complex world that is changing faster with each passing day. Thanks for your consideration.

Sincerely,

Damon Diederich
Privacy Officer / Attorney IV

CC: Erica Weyhenmeyer, Vice Chair
Lois Alexander, NAIC
Jennifer Neuerberg, NAIC
Shana Oppenheim, NAIC
Miguel Romero, NAIC

Attachment: Exhibit A

Exhibit A

STATE OF CALIFORNIA
Ricardo Lara, Insurance Commissioner

DEPARTMENT OF INSURANCE
Legal Division, Government Law Bureau
300 Capitol Mall, 11th Floor
Sacramento, CA 95814

Damon Diederich
Privacy Officer / Attorney III
TEL: 916-492-3567
FAX: 916-324-1883
E-Mail: Damon.Diederich@insurance.ca.gov
www.insurance.ca.gov

March 3, 2022

VIA ELECTRONIC MAIL

Ms. Katie Johnson
Chairwoman, NAIC Privacy Protections (H) Working Group
Bureau of Insurance,
Virginia State Corporation Commission
P.O. Box 1157
Richmond, VA 23218
Katie.Johnson@scc.virginia.gov

SUBJECT: Insurance Privacy Working Group – Suggested Revisions to Model 670

Dear Chair Johnson:

The California Department of Insurance thanks you for taking on the important task of leading the Privacy Protections Working Group. The Department looks forward to further engagement as the Working Group begins the process of revising the NAIC privacy Models. In advance of the development of a new workplan for the Privacy Protections Working Group, the Department would like to offer the following suggestions with respect to revision of the privacy Models. The Department hopes that this letter will provide useful information to you and Working Group leadership as you begin to set an agenda for the coming year.

Summary Overview

- Model 670 is a superior basis for developing a modern privacy rights framework, as compared to Model 672; the Working Group should focus on revision of 670.
    - MDL 670 provides consumers with meaningful Opt-Out right, as compared to MDL 672, which does not permit any opt-out for joint marketing arrangements.
    - MDL 670 provides consumers with access and correction/deletion rights, which are not present in MDL 672.
    - MDL 670 provides regulators with enforcement tools, including penalty powers; MDL 672 contains virtually no enforcement provisions.
    - MDL 670 contains numerous provisions relating to licensee conduct and consumer protection, which are not present in MDL 672, including prohibitions against pretext interviews, restrictions on use of adverse underwriting

information, and requirements to disclose when information is sought solely for marketing or research purposes.

- However, Model 670 is dated, and in need of updating, as discussed below:
- Model 670 definitions need to be broadened, to encompass any personal information in the possession of regulated entities.
    - Includes broadening definition of "Individual" and removal of the "personal, family, or household," distinction contained in the definition of "Insurance Transaction."
    - Clarification of the scope of entities covered by the definition of "Insurance Support Organization," in light of telematic and data product sales.
- Model 670 Privacy Notice requirements must be updated, so that consumers have actual notice of their rights.
    - The "abbreviated" privacy notices received by most consumers do not inform consumers of their rights and generally do not contain significant informative content, other than informing consumers that they are able to request a long-form privacy notice. Consumers should receive actual notice of their rights, as well as actual information about how regulated entities use and disclose consumers' information.
    - The Model should be updated to require additional categories of disclosure, consistent with enhanced disclosures set forth in Model 672, CCPA/Prop. 24, and other, more modern privacy rights laws.
- Model 670, §5 should be updated to address modern forms of electronic data collection for purposes unrelated to the insurance transaction, including via website and app design.
- Model 670 should be updated to include procedures by which consumers may request access to, correction or deletion of their personal information, or means by which the consumer may exercise their rights to opt-in or opt-out.
    - Consistent with CCPA/Prop. 24 and other modern privacy rights schemes, regulated entities should provide web-based access to these services, in a manner which does not require the collection of additional personal information, other than as necessary to verify identity, does not require the requestor to create an account, and does not present other obstacles to the exercise of the consumer's rights.
- Model 670, §13K marketing disclosures should be updated so that marketing disclosures do not occur unless a consumer has opted-in to disclosures; this is consistent with best practices for reducing proliferation of personal information.
- Model 670 should be updated to incorporate antidiscrimination / non-retaliation provisions, so that consumers do not experience unfair discrimination as a result of their election to exercise their privacy rights.

Emphasis on Revising Model 670

It is critical that the Working Group prioritize revision of Model 670. Despite being the older of the two NAIC privacy models, Model 670 provides more comprehensive consumer protections, as compared to Model 672. Both models should be updated, but the Working Group should first focus on making improvements to Model 670.

Model Act versus Model Regulation

Model 670 is the NAIC's Privacy Model Act, meaning it was intended to form the statutory basis for privacy rights of consumers. In contrast, Model 672 is a model regulation, meaning it was intended to provide additional legal requirements in jurisdictions which have already adopted Model 670. Consequently, Model 670 contains a number of consumer rights which are not present in Model 672. While Model 672 is much longer than Model 670, Model 672 only provides enhanced guidance with respect to a handful of privacy rights, consistent with the intent that Model 672 function as additional guidance to jurisdictions which had already adopted Model 670. The fact that Model 672 provides significantly fewer consumer rights is one potential reason why industry stakeholders have been vocal in opposing updates to Model 670 and preferring that the Working Group focus on 672. Moreover, some jurisdictions, including California, are not able to adopt regulations without a basis in underlying statute. Setting forth updated privacy rights as a Model Regulation, rather than a Model Act will pose implementation challenges for member jurisdictions. This is an important reason why the Working Group should prioritize revision of Model 670.

During stakeholder discussions with the prior privacy working group, industry stakeholders raised a number of concerns relating to the structure and implementation of privacy rights. As it currently exists, Model 670 resolves most of the concerns raised by industry. For example, industry stakeholders expressed concern about the potential for insureds' exercise of opt-out rights to hinder disclosures of personal information necessary to transact insurance business, or for reasons of legal compliance. However, all of those issues have been comprehensively addressed in Model 670: Section 13 of Model 670 contains an extensive list of disclosures which are permitted, regardless of a consumer's election to opt-out.

Model 670 sets forth comprehensive privacy rights for consumers. Although it is a few decades old and in need of revision, it is still a more robust means for protecting consumer privacy, as compared to Model 672. Not only does Model 670 contain more consumer rights than 672, it also resolves a number of issues posed by industry stakeholders. Model 672 is riddled with gaps and would require working group membership to reinvent solutions to problems which are already resolved in Model 670. Using Model 670 as a basis for improving consumer privacy rights will result in a better final product, and will facilitate the speedy development of a modern insurance privacy rights scheme.

Right of Access

Model 670 contains a fully developed Right of Access, contained at Section 8 of the Model. The prior Working Group report recommended that consumers be provided a Right of Access, as discussed in Section III of Appendix A of the Working Group report adopted in December 2021. Model 670 contains such a Right of Access, including procedures by which the consumer may request access, means by which the consumer is to be provided access to personal information, timeframes for response by the regulated entity, etc. While there are portions of Section 8 of Model 670 which may benefit from updating, the core Right of Access is already established in the Model. In contrast, Model 672 contains no Right of Access; creating a Right of Access in Model 672 would require Working Group membership to reinvent the wheel, wasting time which may be spent more fruitfully considering other issues.

Right of Correction, Amendment, or Deletion

Section 9 of Model 670 contains a comprehensive implementation of the Right of Correction, Amendment, or Deletion. As set forth in Section IV of Appendix A of the December 2021 Working Group report, membership determined that consumers should be afforded rights to correct, amend, or delete data which is incorrect or no longer relevant. This Right is set forth in detail in Section 9 of Model 670, including procedures by which the consumer may make requests, timeframes for response by the regulated entity, requirements for the regulated entity to notify third-party data recipients of corrected or deleted data, procedures governing a disputed correction or deletion request, etc. Model 672 contains no implementation of the Right of Correction. Again, the Working Group should focus its efforts on revising Model 670 rather than Model 672, in order to avoid duplicating work which was done decades ago.

Pretext Interviews

Section 3 of Model 670 protects consumers against deceptive practices by insurers and their agents. The prohibition against pretext interviews prevents insurers, or their agents and servicing entities, from: misrepresenting their identities, the identity of the person they represent, the purpose of the interview, or refusing to identify themselves. Pretext interviews are allowed in certain cases where the insurer has documented evidence of fraud or criminal conduct. The protection provided by this section of Model 670 is important to ensure that insurance companies deal fairly with their insureds and claimants; however, Model 672 contains no equivalent protection. This is yet another example of how Model 670 provides superior consumer protection, as compared to Model 672.

Marketing and Research Questions

Section 5 of Model 670 sets forth a requirement that insurers and their servicers clearly identify questions posed to the consumer solely for the purpose of marketing or research; this requirement is not present in Model 672. This is an important privacy protection, because it empowers the consumer to determine whether and how much information to give to the insurer. Absent this protection, insurers are free to extract significant amounts of personal information from the insured, even if that information bears no relation to the risk being underwritten. Without identification of questions not required for issuance or servicing of the policy, people will likely provide responses to every question asked of them; this practice promotes data proliferation and diminishes the rights of the consumer. Both Federal and California law currently require that government agencies specify to individuals, in a document called a "Privacy Notice on Collection," the reasons for collection of their personal information, as well as the consequences of not providing any particular item of personal information. Because insurance requires significant amounts of personal information, and is a product necessary for modern consumers, insurers should be under a heightened obligation to disclose to consumers which items of personal information are required for the policy, and which are merely for marketing or other purposes unrelated to the insurance transaction.

Investigative Consumer Reports

Section 7 of Model 670 sets forth consumer rights with respect to development and use of investigative consumer reports. Again, Model 672 does not contain this protection. Insurers are prohibited from using investigative consumer reports, unless the consumer is notified of their right to be interviewed in connection with preparation of the report, and their right to obtain a copy of the report upon completion. It is important that consumers be afforded an opportunity to be interviewed in connection with development of a consumer report, so that the consumer can address any potential inaccuracies, or explain any material which is may negatively impact the consumer. Similarly, the requirement that the consumer be provided a copy of the finished report allows the consumer to verify the accuracy of the contents, ensure that the consumer's input is reflected in the report, and request correction of the report, if necessary. These requirements are all necessary to ensure accuracy and transparency in the use of consumer reports for insurance purposes.

Adverse Underwriting Information

Section 10 of Model 670 requires, in the event of an adverse underwriting decision, that the insurer either inform the consumer of the reasons for the adverse decision, or notify the consumer that the consumer has the right to request information about the adverse decision, as well as inform the consumer about the rights of access, correction, and deletion. Upon request, insurers are required to provide the reasons for the adverse decision, the items of personal information which formed the basis for the adverse decision, and the institutional sources for the

information which led to the decision. These rights are important to prevent unfair discrimination against consumers, and ensure that underwriting decisions are both transparent and based on current, accurate information. However, these rights do not exist in Model 672.

Sections 11 and 12 of Model 670 restrict the ability of insurers to request or use the fact of a prior adverse underwriting decision, or coverage through a residual market mechanism. These protections are necessary to ensure the accuracy of underwriting decisions and prevent unfair discrimination against consumers. However, these protections are not present in Model 672. Section 11 prohibits the insurer from seeking information about prior adverse underwriting decisions, or coverage via residual market mechanism, unless the insurer also requests information about the reasons for the prior adverse decision, or residual market coverage. Section 12 prohibits insurers from basing an adverse underwriting decision on the fact of a prior adverse decision, or coverage through a residual market mechanism, but permits adverse underwriting based on other information received from an insurer responsible for an adverse decision. Similarly, Section 12 prohibits insurers from basing an adverse underwriting decision on information obtained from an insurance support organization whose primary source of information is insurance support institutions, but allows underwriting to be based on information derived from such information. These protections ensure that adverse decisions are based on facts about the insurance risk currently posed by the consumer, rather than the consumer's prior coverage history, or "facts about facts." Again, these protections ensure fairness and transparency in the underwriting process, and prevent unfair discrimination against the consumer.

The protections of Sections 10-12 ensure transparency in adverse underwriting decisions, and that adverse decisions are based on current, relevant, accurate information about the insurance risk posed by the consumer. They are essential to ensure fairness and accuracy in the underwriting process. Unfortunately, these protections are entirely missing from Model 672.

Opt-Out Rights and Joint Marketing Disclosures

Section 13K of Model 670 requires that consumers be provided the opportunity to opt-out of marketing disclosures of their information, while setting limits on the kinds of information that may be disclosed for marketing purposes. In contrast, Section 15 of Model 672 provides that personal information may be disclosed for joint marketing purposes, in which case the consumer has no right to opt-out.[1]

Although Model 670 is an older model than Model 672, Model 670 provides greater protections with respect to marketing disclosures. In context of data proliferation and data breach trends, it is important that consumers be able to exercise control over disclosure of their information.

[1] This is similar to the approach adopted by GLBA at 15 USC §6802(b)(2). However, note that GLBA does not preempt state laws providing greater protection to the consumer, per 15 USC §6807(b).

Decreasing the distribution of personal information is the most certain means to reduce the likelihood that the information will be breached. Therefore, the approach adopted by Model 670 is the better approach to safeguarding consumer privacy.

Investigative and Enforcement Powers of the Commissioner

Model 670 provides insurance commissioners with a robust complement of corrective and enforcement tools, set forth in Sections 14-19. There are no enforcement powers provided in Model 672, other than a vague drafting note in Section 25.

Rights are meaningless, without a way to enforce them. Unless insurance commissioners are granted the ability to investigate violations of privacy rights, bring enforcement actions, and levy fines and penalties, privacy laws are worth little more than the paper they're printed on.

Section 14 of Model 670 grants examination and investigatory powers, enabling regulators to investigate conduct with may violate consumers' privacy rights. Crucially, the exam powers provided in this section grant the commissioner jurisdiction over out-of-state insurance support organizations which affect consumers within the state; absent this special jurisdiction, commissioners would, in many cases, have no ability to investigate out-of-state third-party servicers, even though it is common for a policyholder's information to be handled by out-of-state servicers.

Section 15 of Model 670 permits the commissioner to issue and serve statements of charges whenever the commissioner believes that the conduct of an insurance institution, agent, or insurance support organization violates the provisions of the Model. As with Section 14, Section 15 also contains jurisdictional language granting authority to serve servicers operating outside the commissioner's state. Section 15 further grants the commissioner the power to examine witnesses under oath, receive oral and documentary evidence, subpoena and compel the attendance of witnesses, and compel the production of documents and records. These provisions are all essential so that commissioners may determine, on the basis of factual evidence, whether the requirements of the Model have been violated.

Section 17 permits the commissioner, upon finding that the Model has been violated, to serve those findings upon the violator, along with a cease and desist order enjoining violations of the Model. Furthermore, Section 18 permits the commissioner to assess monetary penalties for violation of the Model, along with enhanced penalties for violation of a cease and desist order of the Commissioner.

Section 19 provides for judicial review of orders of the commissioner enforcing the Model. This is an important Due Process protection, which protects the rights of entities subject to the Model.

Despite the importance of the comprehensive enforcement mechanism provided by Sections 14-19 of Model 670, no equivalent enforcement measures exist in Model 672

Private Right of Action

Section 20 of Model 670 sets forth an individual right of action for violations of the Model. People whose rights under Section 8 (Access), Section 9 (Correction/Deletion), or Section 10 (Adverse Underwriting) have been violated are entitled to apply for equitable relief (i.e.: non-monetary remedies). People whose personal information has been disclosed in violation of Section 13 are entitled to money damages, but those damages are capped at actual damages suffered by the individual.

Privacy is, ultimately, a set of rights about how our personal information is handled. Therefore, it is important that individuals are able to enforce their own rights with respect to how insurers handle personal information. However, Model 672 does not provide this important ability.

Obtaining Information under False Pretenses

In addition to setting forth consumer rights with respect to their information, Model 670 also protects personal information from unauthorized access by third parties, whereas Model 672 does not. Section 22 of Model 670 provides for fines and imprisonment in the event that a person attempts, under false pretenses, to obtain personal information from an insurance entity.

Insurance entities possess a great deal of personal information about consumers and, therefore, are inviting targets for fraud. By providing fines and imprisonment, Model 670 creates a deterrent to people who might otherwise be enticed to obtain information fraudulently.

HIPPA Exemption

As the Department indicated to the Working Group in a letter dated September 7, 2021, a HIPAA exemption is undesirable for a number of reasons. Chief among these are that HIPAA does not require a covered entity to provide consumers with notice of the entity's privacy practices, meaning that consumers are not informed about what information health insurers are collecting about the consumer, or from what sources. Additionally, HIPAA only pertains to "protected health information" ("PHI"), as that term is defined in the regulations; HIPAA does not provide consumers with any rights with respect to non-health personal information possessed by covered entities, meaning that covered entities are free to collect, use, and distribute non-health personal information in the absence of any consumer rights or safeguards. The fact that Model 670 does not contain a HIPAA exemption is yet another reason why Model 670 provides superior consumer protections compared to Model 672.

The Working Group Should Begin with Model 670

Focusing the Model revision process on Model 670 will save significant time and resources. Model 670 was intended as a statutory framework for privacy rights, meaning it is a comprehensive scheme of regulation that addresses many of the concerns identified by stakeholders. Model 672, by its nature as a model regulation, was never intended to create a comprehensive system of privacy rights. While Model 672 has a formidable page count, much of the content therein is devoted to examples and drafting notes, rather than concrete consumer protections. Many of the core rights which constitute a privacy rights scheme are absent from Model 672; inventing those rights from scratch will unnecessarily cost time and resources.

Model 670, while somewhat long in the tooth, is a respectable framework for privacy rights and already contains most of the core rights which should exist in modern privacy rights systems. Therefore, the Working Group should first focus on updating Model 670. Once that task is complete, the Working Group can next turn to Model 672, in order to provide additional context to the rights contained in Model 670.

Updates to Model 670

While Model 670 is a more robust privacy rights scheme compared to Model 672, it is four decades old and showing its age. The state of the art in privacy regulation surpassed Model 670 many years ago. The Department provides the following high-level suggestions for revising Model 670, in hopes that they may assist the Working Group in establishing a work plan. For clarity, these suggested revisions are presented in Section order, rather than order of importance.

Section 2: Definitions

A number of the definitions in Model 670 are underinclusive, or otherwise need revision in order to address modern privacy rights concerns.

Subdivision (J): "Individual"

Model 670 protects the privacy rights of "individual[s]."[2] However, "individual" is defined to only include certain classes of people who have a consumer relationship with the insurer. This may have been acceptable when Model 670 was adopted back in 1980; however, the definition is too narrow in a modern context. Electronic data collection and sharing means that insurance institutions may come into possession of personal information in a number of ways which are unrelated to servicing of an insurance transaction or claim. Personal information may be shared for marketing purposes, as expressly permitted by Section 13K of the Model, or it may be

[2] Note: The definition of "individual" is incorporated into the definition of "Personal Information" in MDL-670, §2T.

gathered in connection with a person's internet use, based on tracking cookies or other methods of online data collection; these uses and means of collection are not clearly covered under the existing definition. Privacy rights should extend to any personal information held by an insurance institution, regardless of how that information came into possession of the institution**.**

Subdivision (M): "Insurance Support Organization"

There is ambiguity in the current definition of "Insurance Support Organization," as it relates to entities which provide data services to insurers. Presently, Subdivision 2(M) defines "Insurance Support Organization" to include "Any person who regularly engages, in whole or in part, in the practice of assembling or collecting information about natural persons for the *primary purpose* of providing the information to an insurance institution or agent for insurance transactions" (Emphasis added). The "primary purpose" language is problematic as it relates to entities which provide data to insurers, because the entity may provide data to entities other than insurers or for additional purposes unrelated to the insurance transaction, and thereby assert that the "primary purpose" of the data collection is unrelated to insurance, notwithstanding that the entity is collecting or disclosing information at the direction of an insurer or producer. For example, an auto insurer might offer a discount based on the insured subscribing to a telematic data collection service relating to the insured's driving habits and/or vehicular "health" information. The telematics vendor would be collecting a significant amount of personal information about the insured's habits and behavior, at the behest of the insurer. However, the vendor may sell their services for purposes other than insurance (e.g.: fleet monitoring, emergency services, etc.), and thereby claim that their business is not for the "primary purpose" of providing information relating to insurance transactions.

Increasing use of telematic and other data products for insurance purposes means that it is important to extend privacy protections to information which is collected at the behest of an insurer, regardless of whether the information is collected via a product or service which may have applications other than insurance.

Subdivision (N): "Insurance Transaction"

Currently, Model 670 only extends privacy protections to "insurance transaction[s] . . . primarily for personal, family, or household needs, rather than business or professional needs."[3] This is a significant limitation on privacy rights, because personal information can be collected in a number of business or other contexts. As currently written, Model 670 provides no protection to personal information which people provide in a number of contexts, which can include workers' compensation, corporate "key-person" life insurance policies, vehicle fleet liability insurance, etc. That personal information is disclosed in a business context does not make it any less

[3] Note that "Personal Information," as defined in MDL-670, §2T, only includes information collected in connection with an "Insurance Transaction," as defined in the Model.

personal to the individual. Therefore, Model 670 needs to be revised to protect all personal information, regardless of the context in which the personal information is collected.

In addition to the personal/business distinction, the current definition of "Insurance Transaction" may be underinclusive with respect to the contexts in which personal information is collected by insurers. Currently, "Insurance Transaction" only includes "determination of eligibility for coverage, benefit, or payment," or servicing of an insurance product. These contexts reflect the state of the world in 1980, and do not reflect that insurers may collect personal information consumers in a variety of contexts online, which may not be included in the current definition. Moreover, insurers may receive information from third parties, related to consumers who have not had any contact with the insurer. The Working Group should ensure that privacy protections are afforded to any information about an individual person, regardless of the context in which an insurance entity came into possession of that information.

Subdivision (T): "Personal Information"

Currently, "Personal Information" is broadly defined in the Model; however, this comes at a cost, as the definition is ambiguous. It may be useful to reconsider the definition in light of more modern definitions of the term. For example, the defined term does not cleanly encompass telematic data. Information which is collected about a person's physical activity, state of their vehicle or home, internet use, etc., may reveal a great deal about a person. Therefore, it is important that any definition of "personal information" expressly include those forms of information collection.

More modern privacy rights schemes tend to either define "personal information" very broadly, so that it is clear that all information about a person is personal information,[4] or provide a general definition supplemented with a specific list of included items.[5] The Working Group may wish to consider adopting this approach when revising the Model definition.

In particular, the currently defined term "personal information" is ambiguous as it relates to sharing of personal information for marketing purposes under Section 13K. As defined in Section 2T, "personal information" means "individually identifiable information . . . from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics." In comparison, Section 13K prohibits marketing-related sharing of "personal information relating to an individual's character, personal habits, mode of living or general reputation." In theory, much of "personal information," as defined, may not be shared for marketing purposes. But because the terms in the Model are ambiguous at best, it is not at all clear what kinds of personal information may not

[4] *See, e.g.:* GDPR Article IV, §1 definition of "Personal Data." Model 672, §4V contains a fairly broad definition of "Personally Identifiable Financial Information," however §4V potentially contains a loophole which exempts personal information obtained or disclosed for marketing purposes.
[5] *See, e.g.:* Prop. 24/CCPA definition of "personal information" at Civil Code ("CIV") §1798.140(v).

be shared for marketing purposes. The Model should be revised to correct this issue, whether through revisions to Section 2T, Section 13K, or both.

Another trend to consider is that some privacy statutes identify "sensitive personal information" as a further category of personal information, and which is subject to additional privacy protections.[6] Defining "sensitive personal information" for purposes of the Model, then restricting use or disclosure of that information, is one potential way to resolve the marketing disclosures issue discussed in the preceding paragraph. For instance, some states are beginning to adopt privacy statutes which permit "opt-out" sharing of general personal information, but require "opt-in" consent for sharing of "sensitive" personal information.

Section 4: Notice of Information Practices

Notice is the foundation of privacy rights because most consumers will not be aware of their rights, let alone exercise them, unless they are provided notice of those rights. Notices provided under the existing Model are inadequate, vague, and uninformative.[7]

One of the main problems with notice requirements in the current Model relates to the "abbreviated notice" provisions of Section 4C. In practice, the vast majority of insurance consumers never receive full notice of an insurer's privacy practices or the consumer's rights, due to the abbreviated notice section. While Section 4B sets forth a variety of informative content to be included in privacy notices, Section 4C ensures that most consumers will never see that informative content. Instead, Section 4C allows for an abbreviated notice in every case. Most egregiously, the "abbreviated notice" is not required to inform consumers of vital privacy rights: abbreviated notices are not required to inform consumers of their right to access their information under Section 8, their right to correct information under Section 9, or their right to opt-out of marketing disclosures under Section 13K. A privacy notice which doesn't inform consumers of their rights is of little value. Abbreviated notices are a major shortcoming of Model 670, and an issue which the Working Group must urgently address.

Another issue with privacy notices under the Model, which may lead to consumers being misled, is the distinction between "selling" of personal information and "sharing/disclosure" of personal information for marketing purposes. Currently, most insurers send out privacy notices which state something like "We don't sell your personal information." While that statement may be factually correct, it belies the fact that most insurers swap information about consumers, and derive valuable benefit from the practice. Consumers read the statement "we don't sell your information," and assume that their information is never leaving the insurer's four walls, which is far from the truth. Therefore, the Model should be revised so that consumers are made aware

[6] *See, e.g.:* CCPA/Prop. 24 definition of "sensitive personal information" at CIV §1798.140(ae).
[7] Note that this same problem exists in MDL 672, §7D, which allows for a short form initial notice with little informative content; moreover, due to the operation of MDL 672, §6B, which eliminates the annual notice requirement in most cases, most consumers will not receive additional notice, beyond the short-form initial notice.

of marketing disclosures, and that notice of those disclosures is made alongside any statement to the effect that insurers aren't "selling" the consumer's information.

Section 4 is deficient with respect to revised privacy notices, an issue which was addressed in Model 672, Section 9. Model 670 should be revised to clarify that no disclosures requiring prior notice and the ability to opt-out can be made, unless the consumer has been provided with accurate notice of those disclosures, and provided an opportunity to opt-out.

While revising the Notice provisions of Section 4, the Working Group should consider the categories of disclosures required to be provided in the Notice. Existing Section 4 of Model 670 requires five categories of information to be disclosed in the Notice; in contrast, Section 7 of Model 672 requires disclosure of nine categories of information. CCPA/Prop. 24, at CIV §1798.130, requires disclosure of nine categories of information, both with respect to a business' collection of information about consumers, as well as a business' disclosure of information about consumers.[8] The Working Group should consider adding additional categories of required disclosure, consistent with the approach adopted in modern privacy rights schemes.

One of the major changes in the world since the adoption of Model 670, back in 1980, is that virtually all businesses now have internet websites. Websites are an ideal means for communicating privacy notices, and other consumer information. While web posting is not an alternative to putting a notice in front of the consumer's eyes, it is a useful way to ensure that notices are always available to the consumer. The Working Group should consider adding web posting mandates to the existing consumer notice provisions in Model 670.

Section 5: Marketing and Research Questions

The policy behind Section 5 is a good one: insurers should inform consumers when collecting information that is not related to servicing the insurance policy, thereby giving consumers the ability to decide how much extra information they are willing to provide.

However, the wording and structure of Section 5 belies its roots in the pre-digital era: Section 5 speaks to "questions designed to obtain information solely for marketing or research purposes," language which is underinclusive in context of electronic data collection practices. Insurance institutions may gather data about people in a number of ways, not all of which are question-based.

The Working Group should consider updating Section 5 to address all insurance data collection, whether or not question-based. In particular, Section 5 should be updated to address data collection relating to internet websites and apps, and how websites and apps are designed. For instance, an insurer's phone app should not require permission to access the consumer's phone

[8] *See:* CIV §§1798.110(c), 1798.115(c), and 1798.130.

contacts in order to work properly. Similarly, an app should not require location information for basic functions, such as finding contact information for the insured's agent; however consumers should expect a diminished experience if they do not authorize certain app permissions.

The same concepts apply to insurers' websites. Websites should disclose if they are using tracking cookies, social media cookies, location information, etc.; website design should allow consumers to utilize an insurer's website, even if the consumer disables tracking/social media cookies or other personalization measures. Notably, website design should allow consumers to exercise their privacy rights without creating an online account with the insurer, or volunteering personal information, beyond the information necessary to confirm the requestor's identity. This is consistent with the practices adopted in CCPA / Prop. 24, which allows people to exercise their privacy rights, without creating an account with the company responding to the request.[9]

Section 8: Access to Recorded Personal Information

The Right of Access is a core privacy right; without a right of access, consumers have no way of learning what information insurers have about the person, or whether that information is correct. While Section 8 of Model 670 already provides a Right of Access, the section should be amended to provide better access to consumers.

For starters, the access provided by Section 8 is premised on the person "reasonably describing" the information sought.[10] This is problematic, because it puts the onus on the consumer to know and describe the information they are seeking. However, consumers have no way of knowing what information a company may possess about the person. This section should be amended to allow a consumer to request access to information, without having to identify what information they are seeking. This approach is consistent with the method adopted in CCPA / Prop. 24.[11]

While Model 670, Section 8 provides consumers with a right to access information about the consumer, it provides little information about how that information has been sold or shared. In contrast, CCPA / Prop. 24, in addition to a right of access to information about the consumer, provides a right to be informed about how businesses have been selling or sharing a person's information, including identification of the types of information shared about the consumer, and the types of entities which received the consumer's information.[12] Section 8 should be updated to provide consumers with a right to request this information. CCPA / Prop. 24 may provide helpful guidance with respect to development of additional categories of information which the consumer may access.

[9] *See, e.g.:* CIV §1798.130(a)(2)(A), relating to the Right of Access, and delivery of information requested by the consumer.
[10] Model 670, §8A.
[11] CIV §§1798.110, 1798.115, 1798.130.
[12] CIV §§1798.115 and 1798.130.

Model 670 again shows its age, in that Section 8 permits consumers to "see and copy" personal information, or "obtain a copy . . . by mail." The Right of Access should be updated such that insurers are required to provide a portal on their website for submitting access requests, and that requested information may be delivered electronically. To facilitate access, insurers should be required to provide consumers with one free electronic copy of their personal information per year, although charges should be permitted for paper copies, or additional requests within a year.

The Working Group may also wish to consider providing guidance with respect to what constitutes "proper identification" sufficient to allow access, as required by Section 8A. California is aware of a number of data breaches which have resulted from online insurance "quote" websites or applications, wherein attackers filled publicly-available information about a consumer into the quote application, which then auto-filled the consumer's driver's license number, or otherwise provided non-public information. While it is important that identification requirements not be so onerous as to be a barrier to access, it is important to instruct insurers and producers that publicly-available info is not sufficient identification upon which to release PII.

Section 10: Adverse Underwriting Information

The right to information about adverse underwriting decisions which currently exists in Model 670, §10 should be expanded. Currently, Section 10 permits insurers to either: provide consumers with the specific reason or reasons for an adverse underwriting decision, or advise the consumer of their right to request that information. The section should be revised so that the consumer automatically receives information about the adverse underwriting, rather than having to request that information. Insurers are already required to provide notice of this information, but it makes sense to provide this information for context, along with notification to the insured of their right to request correction or deletion of incorrect information.

Section 13: Disclosure Limitations and Conditions

The marketing-related personal information disclosures permitted by Section 13 need to be tightened-up, to reflect the problems of data proliferation associated with electronic exchange of information. Regulated entities need to be able to disclose personal information for reasons related to servicing of an insurance policy or claim, or for purposes related to legal compliance; those are all areas where exchange of personal information is related to the insurance transaction, and consumers can and should expect that their information will be disclosed for those reasons.

However, disclosures for marketing purposes are not an essential aspect of the insurance transaction, and should be limited in order to protect insureds' personal information. Specifically, Section 13K should be amended so that marketing disclosures are not permitted unless the consumer has specifically elected to have their personal information disclosed for marketing purposes (i.e.: an "Opt-In" approach). As previously discussed with the Working Group, insurance is a product which consumers are compelled to purchase, unlike social media,

or other products which a consumer may voluntarily interact with. Consumers provide a large amount of very sensitive information to insurers, which is necessary for underwriting purposes. Therefore, an Opt-Out approach is a best practice with respect to insurer marketing disclosures. Moreover, while Section 13K makes some attempt to define categories of information which may not be disclosed for marketing purposes, those categories are vague; a better approach is to specifically define types of information which may not be disclosed for marketing purposes.[13]

Related to marketing disclosures, Section 13(B)(1)(a) should be amended to plug a loophole related to marketing disclosures by third-party contractors of insurers. Currently, Section 13(B)(1)(a) permits those entities to disclose personal information to the same extent as regulated entities, thereby incorporating Section 13K and implicitly meaning that third-parties are permitted to disclose personal information for marketing purposes, without the consent of the consumer. This is a major loophole, and one that the Working Group should address; third-parties should not be permitted to disclose personal information without the opt-in consent of the consumer.

Consistent with limiting personal information disclosures for marketing purposes, Section13L should be amended so that affiliates may only market products of the regulated entity and its affiliates. Marketing disclosure relating to marketing of third-party products or services should require the opt-in consent of the insured.

Sections 18 and 22: Penalty Amounts

The penalty amounts in Sections 18 and 22 are very low, both in terms of per-violation amount, and overall caps, and, therefore, not an effective deterrent against violations of the Model. For example, the $10,000 aggregate violation limit, established in 1980, is worth just over $36,000 in 2022 dollars, according to the Bureau of Labor Statistics CPI calculator. At the current limit of $500 per violation, it only takes 20 violations to reach the penalty cap of $10,000. For context, data breaches typically involve hundreds, if not thousands of individual records. While penalties should not be used to financially impair regulated entities which have suffered a breach, penalties do need to present an effective deterrent. Current penalty amounts are woefully inadequate: $10,000 is statistically insignificant on the balance sheets of many regulated entities. The Working Group may wish to consider penalty cap structures which relate to an insurer's overall financial condition (e.g.: as percentages above a certain amount of net income), as opposed to the current flat rates.

[13] For instance, the Working Group may wish to consider the approach of defining "Sensitive Personal Information" as a subset of "Personal Information," and providing additional protections for SPI; this is the approach taken in CCPA/Prop. 24.

Section 24: Effect of Amendments

Section 24, relating to effective date, needs to be amended, so that newly-adopted amendments to the Model do not effect rights and causes of action which accrued prior to adoption of the amendments.

Anti-discrimination / Non-retaliation

Model 670 does not currently contain anti-discrimination provisions and needs to be updated accordingly. It is important to ensure that consumers are not adversely affected by their information privacy choices. To the extent that regulated entities discriminate against consumers, it should be for reasons related to risk and underwriting, not because a consumer elected to exercise their privacy rights to, e.g.: opt-out of marketing disclosures, or request access to their information or a change in inaccurate information.

As discussed in the Department's September 7, 2021 to the Working Group, implementations of anti-discrimination provisions should specify that they only relate to exercise of privacy rights and do not affect an insurer's ability to underwrite based on actuarially-sound rating factors; similarly, anti-discrimination provisions should not prohibit an insurer from denying coverage when an insured has failed to provide all information typically required as part of the insurer's underwriting practices. However, exercise of privacy rights generally does not relate to the risk borne by the insurer; therefore, availability of coverage and premium charged for that coverage should not be based on elections relating to personal information.

Model 672 contains limited anti-discrimination provisions, but they are not well-developed. CCPA/Prop. 24 contains a comprehensive anti-discrimination statute, at CIV 1798.125. The Working Group should consider borrowing from the CCPA/Prop. 24 provisions when developing anti-discrimination language for Model 670.

Conclusion

For the reasons set forth above, the Department respectfully suggests that the Working Group begin its work by focusing on updates to Model 670. Model 670 provides a far better foundation for development of a modern privacy rights framework, as compared to Model 672. However, Model 670 is somewhat outdated, both in its approach to technology, and in the scope of rights it affords to the consumer. Therefore, the Department suggests that Model 670 be updated as described above. The Department looks forward to working with all of the Working Group membership, towards development of comprehensive privacy rights for insurance consumers.

Sincerely,

Damon Diederich
Privacy Officer / Attorney III

Cc:

Cynthia Amann, Vice Chair
Chris Aufenthie, Vice Chair
Lois Alexander, NAIC
Jennifer McAdam, NAIC

EVERSHEDS SUTHERLAND

THE Committee OF Annuity Insurers
www.annuity-insurers.org

May 30, 2024

Chair Amy Beard (IN)
Vice Chair Erica Weyhenmeyer (IL)
NAIC Privacy Protections (H) Working Group
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, Missouri 64106

Sent via email to: lalexander@naic.org

RE: Request for Written Comments on the Path Forward

Dear Commissioner Beard and Vice Chair Weyhenmeyer:

The Committee of Annuity Insurers (CAI or Committee)[1] appreciates the opportunity to submit the following comments to the 2024 NAIC Privacy Protections (H) Working Group (Working Group) on the best path forward for the Working Group to accomplish its charge to update the NAIC's approach to consumer privacy protections. We applaud the Working Group's continuing efforts on this complex and important issue and its commitment to continuing to work collaboratively over the coming months with consumer and industry stakeholders in order to craft effective, balanced, and pragmatic enhancements to consumer privacy protections that are tailored to the insurance sector.

The Working Group has requested comments in two areas:

1. *Does the Working Group want to continue work on Draft NAIC Privacy Model #674?*

2. *Or should the Working Group revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?*

Our comments below reflect our considered views on these matters and the approach we believe will be best suited to providing meaningful enhanced privacy protections to insurance consumers without causing unwarranted and undesirable disruption to the insurance industry. We also highlight several key issues for the Working Group to consider as it moves forward with this important work. While offering these comments, we would note that we fully support and join in with the comments separately submitted by the joint insurance industry trades.

[1]The Committee of Annuity Insurers is a coalition of life insurance companies that issue annuities. It was formed in 1981 to address legislative and regulatory issues relevant to the annuity industry and to participate in the development of public policy with respect to securities, state regulatory and tax issues affecting annuities. The CAI's current 32 member companies represent approximately 80% of the annuity business in the United States. More information is available at https://www.annuity-insurers.org/.

COMMENTS

1. Does the Working Group want to continue work on Draft NAIC Privacy Model #674?

The Committee strongly opposes continuing to work on Draft NAIC Privacy Model #674. While we are appreciative and respectful of the effort and engagement that has gone into Model #674 to date, we believe the public review and engagement process undertaken by the Working Group to date has revealed a number of significant challenges and fatal flaws posed by the draft that would be impossible to overcome. The Working Group's past efforts to develop Model #674 have confirmed that it is very hard, if not impossible, to adapt language and concepts from generalized privacy regimes to fit the insurance sector. Trying to do so inevitably opens a "Pandora's box" of complex issues and unintended consequences that stem from the fact that other privacy frameworks simply were not developed or designed to work for insurance consumers or businesses. Fortunately, there is a better option: leveraging the NAIC's existing, time-tested, and insurance specific privacy frameworks.

2. Or should the Working Group revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?

The Committee believes that the most effective path forward would be to revise the NAIC's existing Model #672. Doing so would provide a strong basis for enhancing consumer privacy protections without needing to reestablish the foundational concepts of privacy for the insurance sector. Model #672 is already broadly adopted in state legislation, and was developed by the NAIC through significant effort and engagement with consumer and industry stakeholders. Using Model #672 as the basis for the Working Group's current efforts would allow the Working Group to take advantage of all that previous hard work while updating and enhancing consumer protections for today.

Importantly, leveraging existing Model #672, which was developed to implement the Gramm-Leach-Bliley Act (GLBA) for insurance, would help maintain consistency and a level-playing field between the insurance industry and the rest of the financial services sector. One of the Committee's most significant concerns with Draft Model #674, as noted in our previous comment letters, is that it would have placed all insurers at a competitive disadvantage in the broader marketplace for financial products. Using Model #672 as the basis for updating privacy protections for insurance consumers inherently reduces this risk since any enhancements would still be based on GLBA concepts and principles common across the insurance, banking, and securities industries.

That said, we urge the Working Group to continue to be mindful of this important competitive balance as it continues its work, even if it uses Model #672 as the basis for a revised standard. We also urge the Working Group to be mindful of the interplay between any revised version of Model #672 and other financial services sector privacy standards. In many circumstances, Committee members offering variable annuities or other SEC registered insurance products will be simultaneously subject to both the standards established by this Working Group as well as the SEC's separate GLBA privacy standards established in Regulation S-P.[2] Any final revisions to Model #672 should avoid creating conflicting or contradictory requirements with SEC regulations that would make it impossible or impracticable for insurers to simultaneously comply with both standards.

[2]The SEC recently finalized amendments to Regulation S-P, establishing a number of new requirements that will apply to Committee members. *See* https://www.sec.gov/news/press-release/2024-58.

EVERSHEDS SUTHERLAND

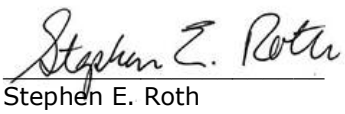
We want to express our appreciation for the opportunity to comment on the path forward for the Working Group, and we look forward to continuing to be a helpful resource as you continue work on this important issue. Please do not hesitate to contact us if you have any questions.

Sincerely,

For The Committee of Annuity Insurers

Eversheds Sutherland (US) LLP

By:



Stephen E. Roth
Mary Jane Wilson-Bilik
Alexander F. L. Sand
Eversheds Sutherland (US) LLP

Arbor Strategies, LLC

Chris Petersen
804-916-1728
cpetersen@arborstrategies.com

May 30, 2024

Commissioner Amy Beard
Chair, NAIC Privacy Protections (D) Working Group
Indiana Department of Insurance
311 West Washington Street
Suite 103
Indianapolis, IN 46204-2787

Dear Commissioner Beard:

I am writing on behalf of a Coalition of health insurers to introduce you to the Coalition and to offer up a resource and assistance as changes are considered to modify the NAIC privacy models. The Coalition represents some of the country's largest major medical insurers and health maintenance organizations. It consists of CVS Health/Aetna, Elevance/Anthem, Cigna Healthcare and UnitedHealthcare, who together provide health insurance and health maintenance organization coverage to more than 200 million members.

We appreciate the opportunity to comment and consistent with our December 2, 2021 letter to the Privacy Protections (D) Working Group (Working Group) we recommend revising Model 672 as the starting point and taking the option provided by industry (Model 672 plus) into consideration. As a bottom line, we believe the following general principals which have guided our thought process on the issues before the Working Group should serve as guideposts for further conversations:

1. Include a properly drafted HIPAA safe harbor to reflect the reality that a robust regulatory framework already exists for HIPAA-protected data;
2. Avoid restrictions on data localization and/or cross-border data provisions which conflict with federal laws and treaties; and
3. Take a cautious and careful approach to privacy rule modifications to ensure achievable compliance and avoid consumer and insurer confusion.

A Properly Drafted HIPAA Safe Harbor is Essential

Inclusion of a HIPAA safe harbor ensures that there is a strong national standard that is consistently applied and enforced on HIPAA-covered entities and other parties complying with the HIPAA privacy rule. It also provides uniformity and administrative efficiencies for insurers

and medical providers and creates certainty for consumers and insurers. We recommend that the safe harbor include the following key components: 1) as provided in Model 672, a safe harbor should apply to any licensee that complies with the HIPAA privacy rule standards; and 2) the scope of the safe harbor should include the entire model or at least those provisions that are also regulated under the HIPAA privacy rule.

The safe harbor language from Model 672 works, and it should be retained. Model 672 provides that '[I]rrespective of whether a licensee is subject to the federal Health Insurance Portability and Accountability Act privacy rule as promulgated by the U.S. Department of Health and Human Services [insert cite] (the "federal rule"), if a licensee complies with all requirements of the federal rule except for its effective date provision, the licensee shall not be subject to the provisions of this Article V."[1] This language has already been vetted and approved by the NAIC. In addition, a significant number of states have also adopted safe harbor language based on Model 672 language.

This approach allows insurance departments to assert jurisdiction over any insurer they determine is not complying with HIPAA. It also provides for consistent enterprise compliance, consumer protections and expectations.

Any Proposed Limitation on Off-Shore Data Sharing Would Be Inappropriate

The ability to transfer data and access personal information across borders is essential to insurers of all sizes. Flows of data are as important to the global economy today as is the flow of goods, services, and capital and can be vital to the interests of globally mobile consumers, in particular with respect to health care delivery and administration. Federal law already sets out the legal landscape in these issue areas. HIPAA does not place any restrictions on this type of sharing so long as proper business associate agreements are in place. Global best practices on cross-border data legal frameworks, permit the free flow of data across borders. Additionally, any restrictions on data flow across borders would violate various provisions of recent free trade agreements including the U.S.-Mexico-Canada Agreement and the U.S.-Japan Digital Trade Agreement[2] and could raise constitutional issues regarding the ability of state law to interfere with federal treaties and the Foreign Affairs power of the United States federal government under Article 1 of the U.S. Constitution.

Changes to the Privacy Rules Must be Done Cautiously and Carefully

Finally, as we noted in earlier comment letters, the United States Department of Health and Human Services ("HHS") forewarns that changes to privacy laws must be done cautiously and carefully. In the executive summary of its June 2021 proposed modifications to the HIPAA

privacy rule, the HHS specifically warns that when done improperly, privacy rules "could present barriers to coordinated care and case management—or impose other regulatory burdens without

---

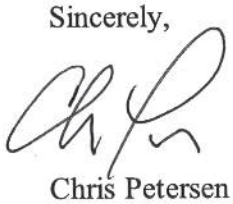
[1] Model 672, §21.

[2] *See for example* AGREEMENT BETWEEN THE UNITED STATES OF AMERICA AND JAPAN CONCERNING DIGITAL TRADE at Article 11 Cross-Border Transfer of Information by Electronic Means "Neither Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means, if this activity is for the conduct of the business of a co vered person." *See also* USMCA Article 17.6: Cross-Border Trade Standstill No Party shall adopt a measure restricting any type of cross-border trade in financial services by cross-border financial service suppliers of another Party that the Party permitted on January 1, 1994, or that is inconsistent with Article 17.3.3 (National Treatment), with respect to the supply of those services.

sufficiently compensating for, or offsetting, such burdens through privacy protections."[3] HHS also warns that the unintended consequences of privacy rules that fail to consider all of the nuances of our health care system could "impede the transformation of the health care system from a system that pays for procedures and services to a system of value-based health care that pays for quality care."[4] The same caution should be applied to any proposed and future changes to the NAIC privacy model.

Thank you for allowing us to introduce ourselves and share our perspective. If you have any questions, please feel free to reach out to me at either (202) 247-0316 or cpetersen@arborstrategies.com. We look forward to serving as a resource and working with the Working Group as it discusses considerations related to NAIC privacy models.

Sincerely,



Chris Petersen

cc: Lois Alexander

[3] Federal Register, Vol. 86, No.12, Thursday, January 21, 2021 at page 6447
[4] *Id.*

May 30, 2024

VIA ELECTRONIC MAIL – lalexander@naic.org

NAIC Privacy Protections Working Group Chair, Amy L. Beard
National Association of Insurance Commissioners c/o Ms. Lois Alexander
1100 Walnut Street
Suite 1500
Kansas City, MO 64106-2197

RE: Comments working group continuing to work on Draft (#674) or to revise existing models (#670 or #672), taking the option provided by industry into consideration

Dear Ms. Beard and members of the Privacy and Protections Working Group:

Nonprofits Insurance Alliance (NIA) is a group of 501(c)(3) nonprofits that insures about 26,000 501(c)(3) nonprofits. We admire the work NAIC has done to creating a draft model law to harmonize the Consumer Privacy Protections for the benefit of consumers. We support the idea of taking the option provided by industry into consideration because industry has the most complete view of what is practical and economically feasible. We also understand and support the point that for the model law to achieve its potential it will have to be broadly adopted by states, so having something most if not all states agree on is important. Keeping all three of these important aspects in mind I suggest that the working group consider two technical methods that can simultaneously help with all three aspects. Specifically, these two technical methods are called differential privacy and homomorphic encryption. Both recently have been identified by the International Association of Privacy Professionals as key components of regimes to achieve the type of results the NAIC model law is seeking. (https://iapp.org/news/a/the-latest-in-homomorphic-encryption-a-game-changer-shaping-up). Although these two technical methods will not solve the entire problem of getting regulators, industry, and consumer groups to agree on what the right law will contain in terms of consumer rights, industry rights and duties, and regulatory oversight, the combination of these two methods can radically reduce the amount of data that is at risk of being compromised, as well as reducing the level of risk to the data that remains. With a reduced amount of data at risk and a reduced level of risk for the remaining data, costs to protect and costs resulting from breaches will both be reduced. There will also be less cost to implement and operate systems for giving consumers visibility into what data companies have and less cost for delete requests or managing consumer preferences as to how that data can be used. These benefits (savings and reduced risks) get multiplied in business environments where data gets passed from the entity directly engaged with consumers (such as a producer, insurance company, or even an employer) to the service providers required to provide the most complete offering and the best choice among multiple options in the market.

Both of these technical methods have been adopted by leading technology companies and the US federal government in just the last 5 years, as they have only now become practical for non-

specialist organizations to develop and deploy as part of their overall solutions. I have included below some examples ranging from use of one technology (differential privacy) in the 2020 US Census to implementations done by a number of leading US companies. The result of adoption by these organizations has been not only to prove these methods out, but also to result in off-the-shelf software libraries that can be used by the non-specialist organizations with a more typical IT department and budget.

A detailed description of how these two technical methods could be implemented within the present eco-system is beyond the scope of this comment letter. However, at a high level the easiest path to getting much of benefit is to use off the shelf software libraries within the existing applications that interface parties to these transactions today. So for instance much like Apple, the US Census Bureau, and Google have put such libraries in their applications that communicate consumer data back to them from a consumer device or web browser, insurance companies or their third party providers can do the same. This is a natural first step since the insurer controls both ends of this transaction and this analogizes to the applications already done by others. So while any time that insurance company shares the data with another organization, say a regulator, the off the shelf software can be used on just the insurer side on the data prior to transmission in ways that gives the regulator what they need to regulate, but that achieves a partial benefit of these technologies, it would be even more beneficial if those upstream counterparties use it as well. But that is not required to get started and get a partial benefit. The next step to get the full benefit would be for other upstream recipients of the data to adopt these technologies to complement what the insurers and their service providers have done first.

Finally, I would mention that there is a large potential to also benefit from the use of these during adjacent operations such as data calls by regulators to insurance companies. So once these methods are being applied in one context, they are very easily leveraged in adjacent contexts.

In summary, differential privacy and homomorphic encryption can radically reduce the amount of personally identifiable information that regulators and companies require to get the important regulatory and business results to serve consumers, while at the same time these methods can drastically reduce the level of risk to the data that is still required.

Respectfully Submitted,

Christopher Reed
General Counsel and Chief Risk Officer
Nonprofits Insurance Alliance
300 Panetta Ave
Santa Cruz, CA 95073

DESCRIPTIONS AND EXAMPLES

DIFFERENTIAL PRIVACY

https://digitalprivacy.ieee.org/publications/topics/what-is-differential-privacy

Example 1 - US 2020 Census used Differential Privacy

https://www.census.gov/library/fact-sheets/2021/differential-privacy-and-the-2020-census.html

Example 2 - IRS and Department of Education, as well as numerous large companies have used Differential Privacy

https://desfontain.es/blog/real-world-differential-privacy.html

Example 3 - California ISO using Differential Privacy to protect consumer data while getting details of consumer energy usage

https://www.recurve.com/blog/solving-energy-data-access-challenges-with-differential-privacy

HOMOMORPHIC ENCRYPTION

https://digitalprivacy.ieee.org/publications/topics/what-is-homomorphic-encryption

Comments on Using Model 674 Version 1.2 versus Industry Draft Revised Model 672
to the NAIC Privacy Protections (H) Working Group

Submitted by Harry Ting, PhD
NAIC Consumer Representative
May 30, 2024

I'd like to thank the Privacy Protections Working Group for this opportunity to submit comments regarding its Model 674 Version 1.2 and the Industry Draft Revised Model 672. I am a strong supporter of the Working Group's goals to add sorely needed privacy protections that are missing from current NAIC models.

I appreciate that several insurance industry groups have taken a constructive approach to formulate a model towards that goal that they can support. Suggesting language to address the challenging areas of data minimization and retention are especially welcome.

Last year, NAIC Consumer Representatives were supportive of the continued development of Model 674. I believe my colleagues would support its continued use by this Working Group. The Industry Draft Revised Model 672 has so many changes to Model 672, that it is essentially also a new model. Whether using it is better than continuing with Model 674 is a matter that Working Group members are probably in the best position to judge.

While we would be pleased to continue to refine Model 674, we can also work with Industry Draft Revised Model 672 (referred to as Model 672R here) if changes are made to it. Here I will limit my comments to the most important general changes that I feel are needed to Model 672R.

1. The top request of all Consumer Representative comments last year was that privacy policies of all licensees should prohibit sharing personally identifiable information unless consumers explicitly opted to share specific categories of information. The justifications for this position are obvious, given the widespread consumer dissatisfaction with the default opt in approach used most often these days. We would be happy to review those reasons again.

2. Model 672R adopts a very different perspective, as is reflected in its statement that "the licensee discloses or reserves the right to disclose nonpublic personal financial information about its consumer to a nonaffiliated third party" unless a consumer opts out. [Section IV.12(1)(a)].

3. It is equally important to protect consumers who are not customers. Consumers who apply for insurance products, but do not purchase, do not get the same protections as Customers in Model 672R.

4. As noted in Section 17 of Model 672R, specification of the protections related to processing of sensitive personal information needs much more definition.

5. Broader coverage of third-party service providers is needed in Model 672R. Model 674 covers information sharing by all third-party service providers, including "a person with whom a licensee does not have a continuing business relationship and does not have a contract, but may have to share personal or publicly [un]available information in connection with a transaction" Model 672R does not have requirements for licensees to control those third-party service providers.

6. Last year, in response to a Consumer Representative suggestion, the chair of the PPWG stated the Working Group would investigate prescribing a privacy policy template that licensees would be required to use. Model 672R provides examples of acceptable privacy policy language, including the current Federal Model Privacy Forms,. Those examples are inadequate to protect consumers' rights, and the suggested personal information categories are too general. As we suggested last year, California's privacy regulations provide much more meaningful categories.

7. Requirements for data minimization and deletion in Model 672R are a welcome addition. Specification of allowable exceptions need to be defined more clearly.

8. Section 29 in Model 972R exempts licensees with fewer than 35,000 resident consumers in a state from several important privacy protections. Why should consumers in those situations get less protection than others? If the concern is the cost to licensees, such an provision would exempt a licensee with 30,000 resident consumers in 50 states, or 1.5 million consumers nationally, which makes no sense.

Again, thank you to the Privacy Protections Working Group for this opportunity to submit brief comments. I and the other NAIC Consumer Representatives look forward to working with you this year to bring your efforts to a successful completion.

IOWA | Insurance Division

GOVERNOR KIM REYNOLDS
LT. GOVERNOR ADAM GREGG

DOUG OMMEN, INSURANCE COMMISSIONER

May 30, 2024

VIA EMAIL

Privacy Protections (H) Working Group
Chair Amy L. Beard, Indiana Insurance Commissioner
Lois Alexander
National Association of Insurance Commissioners
1100 Walnut Street
Suite 1500
Kansas City, MO 64106-2197
lalexander@naic.org

Re: Request for comments regarding future work of the Privacy Protections (H) Working Group

Dear Commissioner Beard and Ms. Alexander,

After the May 15 Open Call of the NAIC Privacy Protections (H) Working Group ("PPWG"), Commissioner Beard invited working group members, interested regulators, and interested parties to submit comments on the following questions:

1. Does the working group want to continue work on Draft NAIC Privacy Model #674?
2. Or revise one or both of the NAIC's existing models, either #670 or #672, taking the option provided by Industry into consideration?

The Iowa Insurance Division would like to thank the members of the PPWG for their careful and thorough work on the issue of consumer data and information privacy. It is in the best interest of regulators, industry, and the public for the PPWG to develop a model law that provides modern, robust protection for consumer privacy.

At the same time, it is important to develop a model law that can be implemented by the industry and that is consistent with existing law. NAIC Privacy Models #670 and #672 have been in place for decades, have been widely adopted by the NAIC members, and offer an effective regulatory framework. Iowa recommends that the PPWG build upon the existing NAIC Privacy Models, rather than continuing to revise Insurance Consumer Privacy Protection Model Law #674. In addition, Iowa agrees that the PPWG should consider the draft revisions to NAIC Privacy of Consumer Financial and Health Information Regulation Model #672 that was recently provided by industry.

Thank you again for your work on this important issue.

Sincerely,

Jordan Esbrook

Jordan Esbrook
General Counsel
Iowa Insurance Division

Insurance Services Office, Inc.
545 Washington Boulevard
Jersey City, NJ 07310-1686
www.iso.com

Stephen C. Clarke, CPCU
Vice President
Government Relations
t 201.469.2656
SClarke@iso.com

May 30, 2024

Attn: Commissioner Amy Beard, Chair
Privacy Protections (H) Working Group
1100 Walnut Street, Suite 1000
Kansas City, MO 64106-2197

Re: Path Forward for the Privacy Protections (H) Working Group

Dear Members of the Privacy Protections (H) Working Group:

Thank you for the opportunity for Insurance Services Office, Inc. (ISO) to provide comments on the path forward for the Privacy Protections (H) Working Group.

For you to best understand our perspective, please note that ISO provides information, including statistics, underwriting and claims information, actuarial analyses, policy language, and consulting and technical services in connection with multiple lines of property/casualty insurance, as well as information about specific properties. Our customers include insurers and reinsurers, as well as agents, brokers, self-insureds, risk managers, financial services firms, regulators, and various government agencies.

Between the two options presented, we do not believe the Privacy Protections (H) Working Group should move forward with draft model law #674. We think the Working Group should look to revise existing model law #672 and we strongly suggest taking the industry option into consideration.

Thank you for the opportunity to share our feedback with you regarding the future of the draft privacy model. Please feel free to contact me should you require additional information concerning ISO's position relative to these matters.

Respectfully Submitted,

Stephen C. Clarke

May 30, 2024

NAIC Privacy Protections (H) Working Group
NAIC Central Office
1100 Walnut Street
Suite 1500
Kansas City, MO 64106

Attn: Lois Alexander, NAIC Market Regulation Manager
Via email: lalexander@naic.org

Dear Chair Beard, Vice Chair Weyhenmeyer, and Members of the Privacy Protections Working Group:

The undersigned joint trades[1] appreciate the Privacy Protections (H) Working Group (PPWG or Working Group) requesting feedback on the appropriate path forward for the working group to accomplish your charges "to draft a new/revised Privacy Protections Model Act to replace/update NAIC models such as Model #670 and/or Model #672."

Privacy is an important matter, and an insurance-specific approach must accomplish several goals simultaneously: reconcile with the context of the insurance industry, align with the broader landscape for other financial institutions[2] nationally, and consider certain state and federal requirements. More specifically, a privacy model law ultimately developed by the NAIC must be operationally practical, reasonable, and workable. It must ensure that its provisions are integrated and work well together and achieve the intended objective of protecting consumers while allowing licensees to meet their business obligations.

In the May 15 email from PPWG Chair Beard, comments were sought on two questions as a basis for helping the Working Group chart its path forward. To streamline your consideration, we have consolidated our joint trade response.

1. **Discontinuing Work on Draft NAIC Privacy Model #674**

The undersigned joint trades strongly oppose continued consideration of NAIC Privacy Draft Model #674. The purpose of updating privacy laws specific to the insurance industry is to align our privacy protection requirements with those key generally applicable privacy requirements in a way that respects the context of insurance. Draft Model #674 would discard the structure insurers have been working under – the one that at a high-level aligns with other financial institutions – and would replace it with something that is being called "radically different." It threatens to introduce significant disruptions for consumers, regulators, and industry players alike.

[1] American Bankers Association *Office of Insurance Advocacy* (ABA); American Council of Life Insurers (ACLI); America's Health Insurance Plans (AHIP); American Property Casualty Insurance Association (APCIA); Consumer Credit Industry Association (CCIA); The Council of Insurance Agents and Brokers (CIAB); Independent Insurance Agents & Brokers of America (IIABA); Insured Retirement Institute (IRI); National Association of Insurance and Financial Advisors (NAIFA); National Association of Mutual Insurance Companies (NAMIC); National Association of Professional Insurance Agents (PIA); Wholesale and Specialty Insurance Association (WSIA).
[2] *See* 15 U.S.C. §6809(3).

2. Leverage NAIC's Existing Model #672; Take the 672-Plus option provided by Industry into consideration

The undersigned joint trades recommend the Working Group revise existing Model #672, taking the 672-Plus option as provided by industry into consideration, for several reasons, including those highlighted below.

Building on Past Success - The NAIC has been a leader in setting standards and expectations for the protection of consumer privacy for decades. Recognizing the unique nature of the business of insurance, the NAIC developed Model #672 to implement the Gramm-Leach-Bliley Act's (GLBA) standards for how insurance companies collect, use, and disclose consumer personal information. Amending the well-established and relatively uniform Model #672 framework with enhanced consumer protections, rather than starting anew, will appropriately bolster the regulation of insurer data privacy and promote consistency for consumers, companies, and regulators. The approach builds onto the well-established and uniform framework. It largely expands the existing requirements, while minimizing disruption of operations that work well today.

Incorporates Many Wide-Spread Key Core State Comprehensive Privacy Law Aspects - The features of the 672-Plus concept have their origin in the state comprehensive privacy laws, which nearly one-third of states have enacted. While they do have some differences, by-and-large these laws are similar and include many of the same components. One message we have heard from regulators is a desire to essentially expand some of these new state requirements to the insurance industry, in a way that makes sense for and is relevant to our industry. The 672-Plus concept incorporates some of the more wide-spread key aspects from those state privacy laws.

For example, its new provisions include: data minimization, consumer requests (for access, correction, and deletion), as well as consumer options to limit (such as for targeted advertising).

Following the approach taken under the state comprehensive laws, the 672-Plus wording would include a limited exemption for licensees that deal with fewer than 35,000 resident consumers - but this draft is more rigorous than the state laws because even entities that qualify for the exemption would still be subject to numerous requirements (including, but not limited to, heightened notice obligations).

Some other changes contemplated in the 672-Plus concept include: modernizing delivery (or access to notice); and expanding requirements relating to contracts with third party service providers.

While the 672-Plus concept represents a positive trajectory, the proposal may need further refinement and fine-tuning, including seeing whether the provisions dovetail as they should. We eagerly anticipate collaborating with regulators and other stakeholders as drafting continues to evolve.

Conclusion

We appreciate the opportunity to have our members' constructive feedback considered and look forward to ongoing and robust dialogue as the drafting process continues. Again, we support:

(1) Discontinuing the wholesale "new wording" that was being contemplated through the Draft Model #674 effort; and

(2) Building from a known and relatively uniform platform by adding -- core key concepts from the state comprehensive laws adapted for the context of the nature of the insurance consumer relationship,

products and services, and regulatory structure – to existing Model #672 to formalize a modernized and expanded 672-Plus model to be available for the states.

Please do not hesitate to contact any of the organizations below with questions.

American Bankers Association: Office of Insurance Advocacy
J. Kevin A. McKechnie
202-320-3306
kmckechn@aba.com

American Council of Life Insurers
Kirsten Wolfford
202-624-2059
kirstenwofford@acli.com

America's Health Insurance Plans
Bob Ridgeway
501-333-2621
bridgeway@ahip.org

American Property Casualty Insurance Association
Kristin Abbott
202-828-7130
Kristin.abbott@apci.org

Consumer Credit Industry Association
John Euwema
630-824-7300
jeuwema@cciaonline.com

The Council of Insurance Agents and Brokers
Joel Kopperud
202-783-4400
Joel.Kopperud@ciab.com

Independent Insurance Agents & Brokers of America
Wes Bissett
202-302-1607
Wes.bissett@iiaba.net

Insured Retirement Institute
Sarah E. Wood
202-469-3021
swood@irionline.org

National Association of Insurance and Financial Advisors
Roger Moore
703-770-8192
rmoore@naifa.org

National Association of Mutual Insurance Companies
Cate Paolino
508-431-0484
cpaolino@namic.org

National Association of Professional Insurance Agents
Lauren Pachman
202-431-1414
Lpachman@pianational.org

Wholesale and Specialty Insurance Association
John H. Meetz
816-799-0863
john@wsia.org

May 29, 2024

Hello fellow Working Group members: let me start my comments by stating that, Yes, I am biased b/c I have been on this working group since 2018, chaired it for a few years and vice chaired it for a few more.

We initially began a review of #670 and #672 with the intent of updating the models to not only reflect 21st century business practices but to also reflect 21st century technological advancements. As you may note, #670 was adopted in 1980 and #672 was adopted in 2000. Not to say they are bad models [evidenced by the 17 states that have enacted some version of 670 and 43 states that have enacted some version of 672] but both models are very out of date. [See the section detailing how to handle information received via fax; or see sections that no longer correspond with various federal acts.]

We tried to update both acts at the same time but quickly found that to be impossible. Please refer to the previous minutes of our presentations and meetings that detail the problems encountered. Please also refer to the 35 page research paper. They will explain the problems encountered and why developing a new model was considered the most expedient way forward.

It seems that if work on the new model is not continued then both of the old models will have to be updated independently while also ensuring that any proposed changes as well as intentions, requirements and definitions are copacetic. That will take A LOT of work. Drafting a new model seems to be the best way to move our work forward.

Also, since several states have recently enacted 'new and improved' data privacy acts the new model #674 has tried to incorporate as many of the new provisions from these new acts as we could. Numerous hours have been expended getting both #670 and #672 drafted into #674. Viewpoints from industry and fellow regulators have been solicited, reviewed and incorporated; a voluminous draft chart shows all stakeholder comments and whether / how stakeholder input was incorporated into draft #674.

Approval was sought and obtained from the H Cmte [our parent group] to develop the new model with the goal of taking the best of both of the existing models and incorporating them into a new model. Please refer to the Model Law Request approved by the H Committee.

I want to draw special attention to the fact that we folded in a lot of the newly enacted legislation from various states; provisions that have addressed topics such as data minimization, transparency, revised notice requirements, the role of third party service providers, as well as ensuring the new model #674 is in sync with the numerous federal acts that pertain to data privacy.

We do need to move forward. As state regulators we should not wait for federal legislators to enact legislation that tells us how to regulate our industry. We need to finish working on a model that is business-practices current, technology-current, and provides sufficient consumer protections. The documents referenced above, along with newly enacted state acts, can serve as a blueprint for moving forward.

So, in conclusion, I would recommend that the Working Group move forward with completing the work on Model #674.

Thanks, CMA

May 29, 2024

VIA EMAIL
Lois Alexander (LAlexander@naic.org)
NAIC Market Regulation Manager II

Amy L. Beard (IN), Chair
Erica Weyhenmeyer (IL), Vice Chair

Privacy Protections (H) Working Group NAIC
1100 Walnut Street,
Suite 1500
Kansas City, MO 64106

Re: Privacy4Cars's Response to NAIC's Request for Written Comments on Path the Forward for Privacy Protections (H) Working Group

Dear Chair Beard, Vice Chair Weyhenmeyer, & Members of the Privacy Protections Working Group:

Privacy4Cars, Inc. ("Privacy4Cars") respectfully submits this letter in response to the Chairwoman's request for public comment regarding the decision to continue drafting NAIC Privacy Model #674, or to revise Models #670 or #672.[1] This question comes at a time in which the privacy and security of data collected by vehicles – including in the specific context of insurance - have reached national attention and have started to result in multiple class action lawsuits.[2] It also comes at a time in which a new federal privacy act is being drafted, including a private right of action remedies. We respectfully submit to the Working Group that, regardless of whether we draft a new model or revise an existing one, the critical issue remains the widespread non-compliance of auto insurance carriers with existing privacy laws (when they exist on a state by state basis)[3] and with well-established "reasonable security" practices, state-specific Data

[1] NAIC Model #670 (NAIC Insurance Information and Privacy Protection Model Act), https://content.naic.org/sites/default/files/model-law-670.pdf; NAIC Model #672 (Privacy of Consumer Financial and Health Information Regulation), https://content.naic.org/sites/default/files/model-law-672.pdf; draft NAIC Model #674 (Insurance Consumer Privacy Protection), https://content.naic.org/sites/default/files/inline-files/Exposure%20Draft-Consumer%20Privacy%20Protection%20Model%20Law%20%23674%201-31-23.pdf

[2] Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies*, The New York Times (March 11, 2024), https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html.

[3] Privacy4Cars, *Laws By Geography*, https://privacy4cars.com/legal-resources/laws-by-geography/.

Security or Data Breach acts,[4] or, for publicly listed companies, obligations under the recent Security and Exchange Commission guidelines.[5] We believe neither approach (drafting a new or revising an existing model law) will result in better consumer protection unless (a) explicit measures are put in place for vehicles, for which data practices and protections are so problematic that they have been defined "privacy nightmare on wheels" by the Mozilla Foundation,[6] and (b) clear enforcement mechanisms are established to ensure that the disincentives to ignore consumer protections outweigh the costs of implementing necessary and overdue changes.

The NAIC Model Law #673 requires:

> *"to establish appropriate standards relating to administrative, technical and physical safeguards: (1) to ensure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of records or information that could result in substantial harm or inconvenience to a customer."*

The sad reality remains: policyholders who experience a total loss accident routinely also experience their personal data stored in the vehicle is (1) left exposed to unauthorized third parties, (2) is unprotected, leading to accidents ranging from identity theft to exposure of their credentials and accounts,[7] (3) despite a growing number of regulators explicitly recognizing the harm and inconvenience those customers can suffer. For instance, Illinois enacted specific legislation aimed at safeguarding consumers against the inherent risks posed by the storage of personal information in vehicles. The Illinois General Assembly in SB-800[8] explicitly recognizes that:

> *(i) due to advancements in technology, personal information associated with consumers is increasingly collected and stored on motor vehicles that function as collateral in secured loans; (ii) the loss or breach of such personal information can cause consumers financial and personal harm and loss; including, but not*

[4] *Id.*

[5] U.S. Securities and Exchange Commission, *Rules and Regulations for the Securities and Exchange Commission and Major Securities Laws*, https://www.sec.gov/about/laws/secrulesregs.

[6] Jen Caltrider, Misha Rykov, and Zoë MacDonald, *It's Official: Cars Are the Worst Product Category We Have Ever Reviewed for Privacy*, The Mozilla Foundation, *Privacy Not Included (Sept. 6, 2023), https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/.

[7] Lora Kolodny and Michael Wayland, *A totaled Tesla was sold for parts in the U.S. but came back online in Ukraine — here's what happened*, CNBC (Aug. 10, 2023), https://www.cnbc.com/2023/08/10/how-totaled-tesla-sold-for-parts-in-us-came-back-online-in-ukraine.html.

[8] Ill.2023 Ill. Pub. Act. 103-0371, § 5(a) (2023).

> *limited to, harm and loss associated with identity theft and loss of privacy; (iii) when motor vehicles are repossessed, it is critical that consumers be protected from such harm and loss; and (iv) collateral recovery practices affect public health, safety, and welfare.*

And consequently declared it wanted to:

> *"ensure that repossession agencies protect motor vehicle collateral consumers from potential harm and loss associated with personal information that is collected and stored on motor vehicles."*[9]

This is not a new issue for this Working Group. Starting in 2021 Privacy4Cars shared statistical studies showing more than 9 out of 10 total loss vehicles capable of collecting sensitive personal information of prior owners and occupants (including minors) actually contain consumers' PI as they are being resold by insurance carriers for salvage. In June 2023, at the Kansas City NAIC conference, multiple members from Insurance Commissioners' offices voiced concern about the sensitive personal data of consumers (e.g., their home address, garage codes, unencrypted text messages, and in newer vehicles biometrics, financial information, user profiles, etc.) being "towed away" after a collision, and questioned the role insurers should have in protecting consumers from data breaches. Those questions remained unanswered.

In order to understand how consumers perceived the role of auto insurance carriers in protecting their data in cars in the case of a total loss, and to measure the attitudes of insurance players towards this rising issue, in March of 2024 Privacy4Cars added a new feature to its https://VehiclePrivacyReport.com website.[10] Consumers, while checking for free what data their vehicle collect, share, and sell could now also enter the name of their auto insurer, see if they have a knows data protection policy for vehicle data stored in cars, and if the carrier does not have a known policy to reasonably protect the personal information stored in total loss vehicles, consumers can ask Privacy4Cars to act on their behalf to ask companies to finally put those "administrative, technical and physical safeguards" in place.

Entirely through word-of-mouth, at the time of this submission almost five hundred consumers submitted webforms demanding better protections from auto insurance carriers! As a result, we have started sending correspondence to insurance companies on their behalf. In most cases, we are not getting any response. Consumers' requests to have their data reasonably protected is

---

[9] *Id*. at § 5(b).

[10] Vehicle Privacy Report™ is an icon-based tool that shows what data manufacturers and popular infotainment apps (SiriusXM, Android Auto, Apple CarPlay, and Amazon Alexa) collect and share or sell. A section called Vehicle Privacy Protections™ was added to help vehicle owners understand what policies their auto finance and insurance companies have to safeguard the personal data in their vehicles – and empower consumers to demand greater protections.

simply going ignored and unanswered, often despite the principles and rules spelled out in past NAIC model laws, as well as to state-specific privacy and data protection laws in effect.

In the few cases in which we got an answer, outcomes for consumers are not better. By means of illustration, we share with the Working Group an anonymized conversation we recently had with the Managing Privacy Attorney from a top three auto insurance carrier. This individual started the meeting by stating how important he thought it would be to protect the personal information of policyholders who suffer a total loss in general, and specifically how if his vehicle was involved in a total loss collision he would certainly be concerned about his data and he would want it to be deleted. "However" he proceeded to state, the company deemed deleting electronic PI from vehicles "not operational in a cost effective way". We don't know what this individual meant specifically, but we want to point out to the Working Group that hundreds of companies, including auto finance companies (from vehicle manufacturers' captives and national banks to credit unions and non-bank lenders), fleets, dealerships, and a few insurance companies have no problem setting, executing, and monitoring policies that accomplish exactly that - tens of thousands of times each month.

The problems for consumers extend beyond the unsecured and unencrypted data abandoned while in the care of insurance carriers in assets they own and put for sale. This Managing Privacy Attorney stated that when consumers placed opt out and data deletion requests (in line with local laws, e.g. under California's Consumer Privacy Act), his team of three was "not equipped to handle these requests via email" and how "overly burdensome" it would be for his team to fulfill these consumer requests. When asked about what other processes consumers could use so the insurance carriers could perform those data subject access requests he did not offer solutions.

What the Working Commission should conclude is that regulated entities are either unaware of their responsibilities, or when they are, they can't seem to be bothered with having policies, procedures, and reporting mechanisms that allow them to lawfully process consumer data.

As long as the financial penalties and individual remedies for violating privacy rights are minimal, businesses may find it economically beneficial to ignore their legal obligations regarding these rights. Therefore, meaningful reform must focus on strengthening enforcement mechanisms to ensure businesses adhere to privacy requests from their customers, thereby protecting the privacy rights of the insured. Refer to Table A for a comparison of the penalties and remedies for violations of NAIC Privacy Models #670, #672, and 674.

Table A

NAIC Model #	Penalties	Individual Remedies
670	≤ $500 per violation ($10,000 cap for multiple violations)	Equitable relief ($0) for violations of Section 8 (Access to Recorded PI) or 9 (Correction, Amendment or Deletion of Recorded PI)
672	Varies under applicable state unfair trade practice laws ("UCL") E.g. California's UCL[11] ≤ $2,500 per violation ≤ $6,000 per certain intentional violations	Varies under applicable state unfair trade practice laws E.g., Cartwright Act gives a private right to sue for actual and treble damages, and preliminary and permanent injunctive relief
674	TBD	TBD

In comparison, the Working Group should consider:

- In New Jersey, Assembly Bill 4723[12] requires dealers to offer all consumers a data deletion of their personal information at lease-end or trade-in. Civil penalties are $500 for the first offense and $1,000 for subsequent offenses.
- The Federal Trade Commission ("FTC") recently warned companies in its blog[13] that it "will take action to protect consumers against the illegal collection, use, and disclosure of their personal data". the blog post said, noting that connected cars and data privacy have been on its "radar for years" including, explicitly, PI left in vehicles. Leaving personal data exposed to unauthorized third parties, the FTC warns, may fall under Unfair or Deceptive Acts and Practices, with penalties of over $50,000 per violation.

We want to thank the Chairwoman and the members of the Privacy Protections (H) Working Group for allowing us to comment and make you aware of the current compliance issues and the

[11] Cal. Bus. & Prof. Code § 17200 *et seq.*

[12] New Jersey Assembly Bill 4723, available at https://pub.njleg.state.nj.us/Bills/2022/A5000/4723_R2.PDF.

[13] Staff in the Office of Technology and The Division of Privacy and Identity Protection, *Cars & Consumer Data: On Unlawful Collection & Use*, FTC Technology Blog (May 14, 2024), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/05/cars-consumer-data-unlawful-collection-use.

importance of making vehicle privacy a lot more explicit and enforceable. We look forward to contributing further and supporting efforts towards meaningful privacy reform.

Sincerely,

Andrea Amico
CEO & Founder, Privacy4Cars

May 30, 2024

Via email to Lois Alexander (lalexander@naic.org)
Manager II, Market Regulation

Commissioner Amy Beard, Chair (IN)
Erica Weyhenmeyer, Vice Chair (IL)
Privacy Protections (H) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106

Re: Path Forward of Privacy Protections Working Group

Dear Commissioner Beard, Vice Chair Weyhenmeyer, and Members of the Privacy Protections Working Group:

On behalf of the National Association of Professional Insurance Agents (PIA)[1], thank you for the opportunity to provide feedback on the most productive path forward for the National Association of Insurance Commissioners (NAIC) Privacy Protections Working Group (PPWG). We appreciate the PPWG's continued attention to the challenges posed by the application of current and nascent technologies and business practices to the NAIC's existing consumer protection regulatory regime. In your request for comments, you set forth two questions, which we address below.

1. **PIA Strongly Discourages the PPWG's Continued Work on Draft NAIC Privacy Model #674.**

PIA has appreciated the work that the PPWG regulators and NAIC staff have invested in the subject of insurance consumer privacy protections over the past two years and recognize and support their continued commitment to achieving a workable model. However, PIA strongly discourages the PPWG from attempting to achieve that goal through the continued development of Draft NAIC Privacy Model #674.

While we had considerable concerns about each draft of the proposed new NAIC Privacy Model #674, we always appreciated, and continue to appreciate, the PPWG's thoughtful consideration of PIA's concerns. In each PPWG meeting in which we participated, we sought to convey the

[1] PIA is a national trade association founded in 1931 whose members are insurance agents and agency owners in all 50 states, Puerto Rico, Guam, and the District of Columbia. PIA members are small business owners and insurance professionals serving insurance consumers in communities across America.

substantial concerns we had about the effect #674 would have on the constantly evolving ways independent agents use data to strengthen the independent agency model and facilitate the growth of their small and mid-sized businesses all around the country. Those concerns have not changed; if anything, in the time since we last communicated with the PPWG, they have grown as independent agents have increasingly come to rely on new technologies, including but not limited to the use of pixels and artificial intelligence (AI).

PIA shares the PPWG's goals of ensuring that consumer data is protected; that consumers know how their data is being used; that they have the right to limit the sharing of their data, other than for insurance-related purposes; and that they are aware of that right and given a chance to exercise it. Empowering consumers to limit the circumstances in which their data may be exploited is valuable, especially as insurance consumer data may be particularly susceptible to exploitation because of the extent to which the purchase of insurance products requires the transmission of potentially sensitive personal information.

All that said, even the most recent iteration of #674 was extremely troubling to our agents. We felt that it was overly broad; we questioned the value of attempting to incorporate tangentially related issues like disclosures around adverse underwriting decisions and oversight of third-party service providers.

We also had concerns about the proposed limitations on the way licensees could use consumer information, which would have been at odds with some independent agents' legal obligations; one example of this was a proposed limitation on licensees' use of information obtained in the process of fulfilling a consumer request to purchase a product. In some circumstances, such uses are mandatory pursuant to state-imposed fiduciary requirements or federally directed insurance programs, like those that provide flood insurance coverage.

2. **PIA Supports the PPWG's Use of NAIC's Existing Model(s) to Produce a Workable and Effective Update to its Existing Regulatory Regime.**

PIA strongly supports the PPWG's efforts to modernize its current regulatory regime by revising its existing models. This approach would allow the PPWG to capitalize on its existing regulatory framework rather than upending it and would benefit regulators, agents, and all licensees by maintaining a level of continuity for all affected stakeholders.

It would also reinforce the NAIC's position as the states' standard-setting body and send a vital message to Congress and federal regulators: The NAIC is the premier regulator of insurance entities, and, in that capacity, it is actively modernizing its consumer data regulatory regime. On behalf of consumers, insurance entities, and state regulators, Congress should not act.

We are still examining the industry-provided updates to the *Privacy of Consumer Financial and Health Information Regulation* (Model #672), as well as the "Core Privacy Issues Quick Look" document, but we are confident that, broadly speaking, a fresh take on #672 would be preferable for agents to the PPWG's continued development of #674.

3. **Conclusion.**

We look forward to discussing the PPWG's path forward with regulators, industry colleagues, and consumer advocates during the upcoming PPWG calls next month. As always, we appreciate the PPWG's recognition that the independent agent community's concerns are often unique, and we are thankful for the opportunity to provide the independent agent perspective.

Please contact me at lpachman@pianational.org or (202) 431-1414 with any questions or concerns. Thank you for your time and consideration.

Sincerely,

Lauren G. Pachman
Counsel and Director of Regulatory Affairs
National Association of Professional Insurance Agents