The Privacy Protections (D) Working Group of the Market Regulation and Consumer Affairs (D) Committee met Aug. 30, 2021. The following Working Group members participated: Cynthia Amann, Chair (MO); Ron Kreiter, Vice Chair (KY); Damon Diederich (CA); LeAnn Crow (KS); T.J. Patton (MN); Chris Aufenthie (ND); Martin Swanson (NE); Teresa Green (OK); Tricia Goldsmith for Raven Collins (OR); Paul Towsen for Gary Jones (PA); and Katie Johnson (VA). Also participating were: Rick Cruz (MN); and Don Beatty (VA).

1. **Adopted its July 12 Minutes**

The Working Group adopted its July 12 minutes as amended with the revision requested by Karrol Kitt (University of Texas at Austin) to change the phrase “credit card” to “debit card.” Mr. Kreiter made a motion, seconded by Mr. Swanson, to adopt the Working Group’s July 12 minutes (Attachment XX). The motion passed unanimously.

2. **Heard an Update from the Summer National Meeting**

Ms. Amann said consumer data privacy was one of the discussion topics during the Summer National Meeting in Columbus, OH. She said the Innovation and Technology (EX) Task Force discussed the ownership of consumer data prior to the update she gave to the Task Force on the activities of the Working Group. She said the discussion about the ownership of consumer data continued during her report to the Market Regulation and Consumer Affairs (D) Committee, which is the parent committee of the Working Group. She said there was also a discussion about possibly creating a new lettered committee that would be known as the (H) committee to oversee cybersecurity issues. However, she said the appointment of a new lettered committee and the assignment of the consumer data ownership issue as a charge were both delayed for further consideration and determination at a future date. She said the Working Group was praised for its work to date and encouraged to complete its charges as written by the assigned due date, even if it required an acceleration of its meeting schedule. Chris Petersen (Arbor Strategies LLC) said data ownership was last discussed following the most recent update to the Privacy of Consumer Financial and Health Information Regulation (#672), which he said he would find and share with the Working Group. Ms. Amann said there was a discussion of data ownership along with some definitions for consideration by the Working Group in the National Institute of Standards and Technology (NIST).

3. **Heard an Update on State Privacy Legislation by NAIC Legal Staff**

Jennifer McAdam (NAIC Senior Counsel) said many consumer privacy rights can be traced back to federal implementation of the Fair Credit Reporting Act-FCRA, to which NAIC Model #670 is most similar. She said each year since the California Consumer Protection Act (CCPA) was adopted, states have introduced similar legislation; and she noted that updated state legislation charts are posted to the Working Group’s Webpage under the documents tab. Ms. McAdam said since California was the first, and is the most comprehensive thus far, that it is also included under the documents tab within one of the comparison charts completed by the NAIC Legal team: a) the Model #670 to the CCPA Privacy Comparison; and b) the Gramm-Leach-Bliley Act (GLBA) to Health Insurance Portability and Accountability Act (HIPAA) Privacy Comparison. She said some of the pending state legislation has gone even further than CCPA to look more like the General Data Protection Act (GDPR). Ms. McAdam said there was not much to report regarding movement on state privacy legislation as most of the bills proposed were not adopted. However, she said Colorado and Virginia were the exceptions as both passed consumer privacy legislation in 2021. Ms. McAdam said the Virginia Consumer Data Protection Act (CDPA) goes into effect Jan. 1, 2023; applies to companies doing business in Virginia or marketing to Virginia residents; and gives consumers the right to access, correct, delete, and opt out of the sale and processing for targeted advertising purposes. She said that the Virginia law is like the CCPA in some areas, but like the GDPR in others. Ms. McAdam said it has no private right of action so enforcement is under the state Attorney General. She said the Colorado Privacy Act (CPA) goes into effect July 1, 2023. She said the Colorado law is not as stringent as the CCPA, but, that it is more stringent than the Virginia CDPA. Colorado CPA also gives the Attorney General’s office the right to establish regulations. Ms. McAdam said Ohio has pending legislation that is not as extensive as California, Colorado, or Virginia. She said it has no private right of action, but it does have a safe harbor for industry. Ms. McAdam said the Uniform Laws Commission (ULC) recently adopted the Uniform Personal Data Protection Act that may be finding its way into state legislation. She said the Legal Division will continue to follow state data privacy legislation as a few states will still be having legislative sessions that run through the end of the year.
4. Heard an Update on California Proposition 24

Mr. Diederich, California’s Acting Privacy Officer, said Proposition 24 is a follow-up to the CCPA that was developed to counter proposed legislation that was perceived to weaken the CCPA by adding some protection rights to data subjects. He said when it becomes effective Jan. 1, 2023, it will add some additional data rights and protections for consumers. He said the bigger differences are a limitation on the collection and use of personal information to certain categories and specific uses, which are disclosed to the data subject at the time of collection. He said there is a requirement for specific disclosures relating to sensitive personal information as defined in the proposition and for retention periods for each category of personal information. He said it must be reasonably necessary and proportionate with respect to the purpose of data collection that are disclosed to the consumer. He said businesses selling or disclosing personal information are required to sign a legal contract with any recipients of that data, such that the recipient would adhere to these set disclosure limitations on data use in terms of the proposition generally. He said there is a requirement for the adoption of security procedures, so the right to limit use and the disclosure of sensitive personal information is a major addition, and a major set of rights, which are provided on top of the CCPA. He said this grants a consumer the right to instruct businesses to limit user disclosure of sensible, sensitive, personal information to perform services expected by the average consumer requesting those types of services. He said sensible, sensitive, personal information includes social security numbers; driver’s licenses; passports; financial account information; account log ins; geo locations; ethnic origin; religious or philosophical beliefs; union membership; contents of mail, email, or text messages; genetic data; health information; and information about your sex life or sexual orientation. He said to the extent that businesses disclose a consumer’s sensitive personal information to third-party users, companies are required to provide notice to the consumer of that disclosure to the third-party user and give the consumer notice of the right to limit disclosure to that user. He said there is also an existing right of non-retaliation that could be considered as a consumer right of non-discrimination. He said there is new protection to employees, job applicants, and independent contractors of the business; a clarification that the non-discrimination provisions do not prohibit loyalty or other rewards programs; an expanded right of deletion and correction of inaccurate information; a clarification for businesses disclosing personal information after informing recipients; and a clarification that information third parties and vendors. He said there is a requirement for a web-based registration of request to exercise privacy rights; and for any information disclosed, the consumer must be provided with a commonly used machine-readable format that is readily understandable and that applies to the insurance industry. Ms. Amann asked if there had been a lot of opposition to the proposition or if it is just working its way through the process. Mr. Diederich said California is still in the rule-making phase, so it is too soon to tell.

5. Exposed the First Working Group Exposure Draft of the Privacy Policy Statement with Comments Incorporated

Ms. Amann said the next item on the agenda is to walk through the exposure draft of the privacy policy statement (Attachment XX) that was distributed Aug. 26. She said the document begins with the Working Group’s 2021 charges and the work plan it has followed since the first Working Group meeting in November 2019. She said following an initial delay due to the pandemic, the six consumer data privacy protections identified as gaps per the analysis in the work plan were discussed by the Working Group during meetings in November 2020 and March, May, June, and July 2021. She said Page 1 of the exposure draft listed the rights identified in the NAIC Member-Adopted Strategy for Consumer Data Privacy Protections received through the Market Regulation and Consumer Affairs (D) Committee as:

1. The right to opt out of data sharing.
2. The right to opt in to data sharing.
3. The right to correct information.
4. The right to delete information.
5. The right of data portability.
6. The right to restrict the use of data.

Ms. Amann said a format template with separate outline sections for each of these six consumer categories has been posted, presented, and discussed at Working Group meetings. She said 18 sets of comments received from members, state insurance regulators, and interested parties were copied and pasted into the format template without labels, and in no order, for each of these rights. She said Pages 2 and 3 list the states that have adopted Model #670, Model # 672, and the Insurance Data Security Model Law (#668). She said the consumer privacy protections addressed in each of these models are also noted. She said Pages 3 and 4 include a review of privacy rights in the GDPR and the CCPA. She said Pages 4 and 5 review state privacy legislation. Links to comparison charts identify gaps in current state and federal laws and rules between the GLBA and HIPAA, as well as between Model #670 and the CCPA. Ms. Amann also said since this material had already been vetted by the Working Group in prior meetings, the Working Group was asking members, interested parties, and interested state insurance regulators to...
review the combined material and submit comments in the following manner as the Working Group proceeded to meet on a bi-weekly basis going forward:

- Segment One: The right to opt out of data sharing, as addressed in Pages 5–29 by Sept. 7, to be discussed at the Sept. 13 Working Group meeting.
- Segment Two: The right to opt in to data sharing, as addressed in Pages 29–32 by Sept. 20, to be discussed at the Sept. 27 Working Group meeting.
- Segment Three: The right to correct information, as addressed in Pages 32–36 by Oct. 4, to be discussed at the Oct. 11 Working Group meeting.
- Segment Four: The right to delete information, as addressed in Pages 36–39 by Oct. 18, to be discussed at the Oct. 25 Working Group meeting.
- Segment Five: The right of data portability, as addressed in Pages 39–46 by Nov. 1, to be discussed at the Nov. 8 Working Group meeting.
- Segment Six: The right to restrict the use of data, as addressed in Pages 46–50 by Nov. 15, to be discussed at the Nov. 22 Working Group meeting.

Ms. Amann said this schedule would be posted to the Working Group’s web page. She said comments could be submitted on the entire draft, any part of the draft, or any of the segments at any time. She said comments received and discussed would be incorporated into the exposure draft, as needed, to complete the Working Group’s charges.

Shelby Schoensee (American Council of Life Insurers—ACLI) said she and Kristen Abbott (ACLI) want to thank the chair and the Working Group for the exposure document. She said the document was very helpful; it was clear how much work went into it and how many years of history were involved. She wanted to confirm that the exposure document was a draft that included historical considerations, input received from interested parties and state insurance regulators, and recommendations introduced and discussed at the end of the document and at the end of each section as the Working Group moves through its discussions during the accelerated meetings. She said it sounds like the Working Group was hoping to get more input on the exposure document throughout those meetings, and at the end of the process, the Working Group would make sure that the recommendations flow from the revised document. Ms. Amann confirmed this was the plan. Ms. Schoensee said the ACLI just wants to make sure that it could communicate that effectively to its members to get constructive feedback to the Working Group throughout the process. She said ACLI members were excited to work on the privacy policy statement. Ms. Amann said comments submitted do not have to be formal, but they can just be bullet points of items to discuss, as the Working Group is more interested in getting a good flow of discussion going than it is about the formality of comments.

6. Received Additional Comments from a Consumer Perspective of Data Privacy

Harry Ting (Health Consumer Advocate) said the nine principles (Attachment XX) he formulated were based upon review of the meeting materials and privacy materials used in the real world. He said he hoped the principles would help the Working Group when evaluating consumer data privacy models. He said he took a different perspective from that encompassed in the six categories identified by the Working Group as rights. For the right to delete, he said his principles would mandate the deletion of certain personal information when it is no longer needed rather than provide a right to delete that a consumer would have to request to activate. He said only insurance-related businesses that need unpublished personal consumer data to complete insurance transactions should be allowed to collect such data. He said lead generating companies that only collect such data to sell it should not be allowed to collect the data, especially when the data is being sold to other businesses that do not meet this criterion. He said he ran across this type of lead generating company last year when he was doing some secret shopping for health insurance online and logged in to search on health insurance. He learned that the company was sharing his information with over 1,700 different companies when he was given a link to the companies that had been given his data. He said most had nothing to do with health or any other insurance. He said insurers and related parties should only keep data for as long as it is needed for the transaction or to meet regulatory requirements; when that data is not needed anymore, it should be deleted. He said businesses should not transfer or sell data to other business entities, whether they are related or not. He said if such a transfer or sale is not essential for the insurance transaction, it should be the consumer’s choice whether to be contacted and provided with that information and only if the consumer wants information on the services or products that she or he did not request. He said the fifth principle ensures the accuracy of data that has a material impact on the consumer’s purchase or receipt of services because it ensures the consumer can verify whether the data being used is correct, as we all know errors in data can occur when it is out of date or when it is misreported by third parties or data entry mistakes occur, and the insurers can develop a standard data set format to meet this requirement to minimize the burden of this requirement. He said he knew from personal experience in looking at credit reports, where he found errors in the data, and when he tried to correct it, it was so frustrating.
that he gave up. He said the accuracy of a consumer’s data needs to be confirmed prior to the transaction occurring. He said if the company has a third party confirm the data, the initial company should still be responsible for spot-checking the accuracy of consumer data and the corrections thereof that have been done by the third-party user. He said insurers should never use information from consumer tracking programs that use cookies or other software tools to collect data on a consumer's online activities. He said even if the consumer permitted the use of that software on their electronic devices, it is not reasonable to assume that consumers will be aware of what is being collected and how it is being used nor that consumers were happy companies had that information. He said exceptions to these principles should only be allowed to meet federal or state requirements, and consumers should be notified when such exceptions occur so they can be informed as to what unpublished personal data was used and why. He said it should be the responsibility of regulatory authorities to ensure that these requirements are met and that sufficient penalties are established to incent compliance because consumers do not have the tools or the expertise to investigate compliance on a case-by-case basis. He said these nine points were meaningful consumer expectations that he hoped the Working Group would consider in its deliberations. Ms. Amann said he raised some valid points that the Working Group would need to consider.

Brenda J. Cude (University of Georgia) said she is not representing any other consumer representatives, and these are her own thoughts after going through the exposure document a couple of times over the weekend. She said she wants to talk briefly about some reactions to what is in the exposure document about opting in and opting out, consumer notices, and the right to delete information. She reminded everyone how difficult it is for consumers to understand the implications of that choice. She said if she were to have the option to opt out, she assumed that it would only be for sharing or selling data to third parties. She said consumers do not know the difference between company affiliates and third parties. Consumers also do not know what the costs and benefits to them are of sharing or not sharing because there is no research. Dr. Cude guessed that most consumers would have a default position. Either they would always opt out based on principle, or they would never opt out, probably because they do not know how a choice to opt out could limit their opportunities to work with a company. Dr. Cude said she does not know what the implication of this is, but it is a very difficult choice for consumers. She said whether a consumer chooses to opt in or opt out is not a decision consumers can make given the incomplete information one has. As it stands now, the other point she wanted to make about this is that, while we probably all see the HIPPA language as something very different than what would apply to car insurance, consumers do not necessarily think of it that way. To them, insurance is insurance; so why should there be one standard for one type of insurance (TOI) and a different standard for another TOI. However, even as Dr. Cude was saying this, she realized she was not saying the standards should apply exactly, but maybe the framework should apply. Therefore, if the default is that consumers opt out of data sharing for any purpose not linked to treatment, payment, or health care operations, or as otherwise required by law, she asked if there might be a parallel for other TOIs that we opt out of data sharing for any purpose not linked to fill in the blank underwriting claims. She said she is not sure what that list would be, perhaps with specific opt-in options for other purposes. Therefore, consumers must opt in for the sale of specific types of information, or they must opt in for the disclosure of information obtained from third parties. Dr. Cude said she also was struck by what seemed to be industry arguments at the end; therefore, it would be too difficult to implement an opt-out standard. She said the health insurance industry has obviously figured it out, and there might be a lot of protocols from the consumer reporting industry that could be transferred to insurance (e.g., how a consumer would verify the identity of an individual who is requesting their own credit).

Dr. Cude reminded the Working Group to resolve the issue of consumer notices by utilizing research guided by professionals with expertise about notices or modifications regarding their use by consumers, but she does not think state insurance regulators have the legal authority to change them. If they do, she said she would like to see that same research-driven approach because she believes a conversation about sample clauses has value. She asked the Working Group to remember that its key strengths are listening and being heard; and sample language is helpful to industry; however, it is also helpful to consumers if it provides consistency to consumer communications. She said sample language needs to continue to be used and should be adopted widely so it benefits consumers as well as industry. She said there is some conversation about consumer use of electronic sources; and while she agrees that much has changed in the intervening years since the NAIC first started talking about this, she also agrees with the value of just-in-time communications that are likely to be delivered electronically. However, she does not want the Working Group to forget that not all consumers have the option to receive information electronically, and some consumers just prefer not to. She said she wants to make sure that the Working Group keeps that in mind and allows, or maybe even requires, that consumers have the choice to continue to receive paper copies. She said if the Working Group goes in the direction of allowing electronic delivery, she does not know why that should be available to consumers only after they become policyholders. She said the option should be posted to the website for consumers to consider as they select an insurance company. She said she spent some time thinking about what it means in the context of insurance to have the right to delete information. She said she readily admits she does not know much about state laws requiring retention of information, but she suggested that for insurance, there is a distinction between deletion and what she would call deactivation. She said the data would have to be retained, but it could not be used in any way after the retention period has ended. She also suggested that the
Working Group think about what deletion means in the insurance context. She said she also does not know what portability means in the context of insurance, but she looks forward to the Working Group’s conversations about that. She said she would put her comments in writing in the hope that they are somewhat transparent at that point. She said she was thinking about the data privacy issue in the context of data portability as she assembled information for a company underwriting her property insurance, and again when she had to do it all over again to get a different quote from another company, as opposed to somehow having access to the data on her property.

Ms. Amann said this portability discussion is helpful, and the example that comes to mind on the commercial side is when a consumer gets a loss run form that can be taken from carrier to carrier. She said the Working Group would make sure to have some good examples of what portability means in the context of consumer data privacy protections. Birny Birnbaum (Center for Economic Justice—CEJ) thanked Dr. Ting for the principles that he set out, and he asked whether those principles were informed by any principles that were developed by consumer or privacy organizations like the World Privacy Forum (WPF), the Electronic Frontier Foundation (EFF), or the CEJ or if he relied on any other parties to develop those principles. Dr. Ting said the nine principles were purely his own reactions to reading about the materials that were submitted to the Working Group and thinking about his own personal values about the use of personal data. Therefore, he said it is not based upon any other sources. Mr. Birnbaum said a lot of what Dr. Ting said is consistent with leading digital rights and privacy organizations that come up with recommendations for the Working Group.

Mr. Petersen said what is viewed as portability in the exposure document is an issue that needs to be resolved. He said portability in the health insurance world is the ability to go from one insurance company to another with no new pre-authorization, even though the term is just used but has not been defined. He said it would be helpful if everyone discussing it in this Working Group were using the same definition for portability. He said Dr. Cude referred to not knowing what retention was, but that she had probably read some materials on it. He said retention is different than authorizing one insurance company to transfer a consumer’s information over to another for either underwriting or claims processing. He said that is a totally different sort of transfer of information that is done for completely different reasons. He said the company transfers the information so it can be used to underwrite or pay a claim while keeping it in the company’s records. Ms. Amann said for the purpose of the exposure draft, a succinct definition will need to be developed, or perhaps it must be determined that portability may not be the best term to use. However, she said this has been a good conversation because it helps to clarify that it is not only about portability from the health perspective, but from a consumer’s general perspective, who has collected all necessary information that the consumer now wants to share with various insurers with a request for a quote. The consumer does not want to fill out 18 different forms to get those quotes. Dr. Cude said it relates to who owns the data, with the concept being it is my own personal data, and I should have access to it. Mr. Diederich said portability is seen as a subset of the right of access because access is the overarching right. He said it is information about you personally and you have a right to access it, which means portability would mean how that data is given to you. It should be in an easily machine-readable format that is understandable because consumers like it that way. Mr. Diederich said the right of access is what the Working Group is trying to define, and portability refers to certain aspects of that right. Ms. Amann said that is how she had always understood portability, but it is good to know that it needs some work. She said the Working Group wants to be clear about its intention, which is to not be specific by line of business, while recognizing that health has a great deal of guidance through HIPPA and other provisions. Mr. Petersen said that is a good reminder that the health insurance industry is heavily regulated by the HIPAA privacy rule, and that rule preempts state law. He said he believed people were leaning towards an exemption if the company complies with HIPAA, and he believed it might be easier if companies have that exemption because then the Working Group could make rules that are not as complicated for the rest of the industry, while leaving health insurers to tackle the extensive HIPAA privacy role to which they are already subjected.

Angela Gleason (American Property Casualty Insurance Association—APCIA) said the APCIA’s comments and observations include high level examples about how the restrictions and requirements for data align with the relationships of the parties and the products, as well as how that works together. She said the APCIA did not like use of the word “right” in discussions, but it looks forward to working through discussions about that during the Working Group process. Ms. Amann asked everyone to remember that the Working Group was instructed to focus on the six consumer rights and use them to provide recommendations along with the basis for the recommendations for consideration by the Market Regulation and Consumer Affairs (D) Committee. She also asked the Working Group to recognize that the recommendation would not be the conclusion, but there would still be model work to do in 2022. She said once the Committee has blessed the definitions and recommendations, the Working Group would pick up where it left off with revisions to Model #670 and Model #672 if that ends up being the will of the group, or it will develop a new model if so directed. Therefore, she said there would still be plenty of opportunities to comment on whatever is concluded or recommended going forward. Wes Bissett (Independent Insurance Agents and Brokers of America—IIABA) asked if the Working Group’s goal is that the deliverable to the parent committee by the end of the year will essentially be plain language recommendations on these six issues, and not necessarily proposed statutory or regulatory
language that would effectuate whatever outcomes the Working Group recommends. Ms. Amann said when Model #670 and Model #672 were last revised, several items were identified as outdated from a business or technology perspective, but the Working Group did not want to spend a lot of time wordsmithing the function or right. Lois E. Alexander (NAIC) said the expectation is that the deliverable will be the privacy policy statement with a comprehensive report about what was discussed, as well as the reasons why the Working Group supports the recommendations given. She said the report will not be just a paragraph with Working Group recommendations because that is something that could be done any time. She said the reason why the Working Group is going through this entire process is to get feedback from all stakeholders so a comprehensive report could be formulated for the parent company. Mr. Bissett said that explanation helps because stakeholders have struggled to understand the purpose of the privacy policy statement and how to respond to it, but it sounds like the privacy policy statement is ultimately the center of gravity for recommendations on the six issues or rights on which stakeholders can focus their efforts. Ms. Amann said Working Group discussions going forward will be used to tweak the privacy policy statement and recommendations report based on the better understanding and clarification obtained through consensus on the document. She said the document is long and it will probably get a little longer, but due to an ambitious schedule, she recognized that everybody would not be able to make conference calls as frequently as they are scheduled. However, she asked stakeholders who have questions or comments to submit, but who are unable to make the call, to please let Ms. Alexander or himself know, and they would be glad to raise the points on your behalf. She said if anyone misses a call and has questions, to please reach out and call either of them as they are always glad to bring anybody up to speed on what was discussed, as well as how or why a decision was made. Ms. Amann said the next Working Group meeting is scheduled for Sept. 13.

Having no further business, the Privacy Protections (D) Working Group adjourned.

W:\National Meetings\2021\Fall\Cmte\D\Privacy Protections\Aug 30 Call\Privacyprot_083021_Min.Docx