INNOVATION, CYBERSECURITY, AND TECHNOLOGY (H) COMMITTEE

© 2023 National Association of Insurance Commissioners

Draft: 8/30/23

Innovation, Cybersecurity, and Technology (H) Committee
Seattle, Washington
August 13, 2023

The Innovation, Cybersecurity, and Technology (H) Committee met in Seattle, WA, Aug. 13, 2023. The following Committee members participated: Kathleen A. Birrane, Chair (MD); Michael Conway, Co-Vice Chair (CO); Doug Ommen, Co-Vice Chair (IA); Karima M. Woods (DC); John F. King (GA); Gordon I. Ito represented by Kathleen Nakasone (HI); Dana Popish Severinghaus represented by KC Stralka (IL); Chlora Lindley-Myers represented by Cynthia Amann (MO); Troy Downing (MT); Jon Godfread (ND); Adrienne A. Harris represented by John Finston (NY); Judith L. French (OH); Carter Lawrence represented by Stephanie Cope (TN); Kevin Gaffney (VT); and Mike Kreidler represented by Byron Welch (WA). Also participating were: Lori K. Wing-Heier (AK); Wanchin Chou (CT); Michael Humphreys (PA); and Katie Johnson (VA).

1. <u>Adopted its 2023 Spring National Meeting Minutes</u>

Executive Deputy Superintendent Finston made a motion, seconded by Commissioner King, to adopt the Committee's March 22 minutes (*see NAIC Proceedings – Spring 2023, Innovation, Cybersecurity, and Technology (H) Committee*). The motion passed unanimously.

2. <u>Adopted the Reports of its Working Groups</u>

   A. <u>Big Data and Artificial Intelligence (H) Working Group</u>

Superintendent Dwyer said the Big Data and Artificial Intelligence (H) Working Group met the morning of Aug. 13 during the Summer National Meeting. Related to the Working Group's artificial intelligence (AI)/machine learning (ML) survey efforts, Superintendent Dwyer said the Working Group received a report from Commissioner Gaffney summarizing observations from the home insurance AI/ML survey. She also reported that the Working Group heard a presentation on generative AI from Casey Kacirek (Deloitte) and David Sherwood (Deloitte). The presentation addressed how generative AI currently works, the emerging capabilities of generative AI, how to measure and mitigate AI risk, insurance industry examples of the benefits of AI, and common AI terms and definitions.

   B. <u>Cybersecurity (H) Working Group</u>

Amann stated that the Cybersecurity (H) Working Group met March 7 in lieu of the Spring National Meeting. Since then, the drafting group of state insurance regulators has been meeting to develop a Cybersecurity Event Response Plan (CERP), which will be a useful resource for regulators with less experience but who are charged with leading a department's response to cyber events at regulated entities. The Working Group requested input from the public and received input from trade associations, including the National Association of Mutual Insurance Companies (NAMIC), the American Council of Life Insurers (ACLI), and the American Land Title Association (ALTA). Amann also thanked the states of Connecticut, Kansas, Illinois, New York, North Dakota and Virginia for their contributions to the CERP drafting efforts. The Working Group will also continue monitoring federal and international developments. The Working Group anticipates a meeting in September based on the current progress of the CERP drafting.

© 2023 National Association of Insurance Commissioners

C. E-Commerce (H) Working Group

Director French reported that the E-Commerce (H) Working Group chairs have now met several times to discuss the Working Group's next steps and to give NAIC staff guidance on drafting a framework that would serve as a guide for states looking to modernize their regulatory requirements. NAIC staff are currently in the process of scheduling a meeting to present the draft framework for comment, and the Working Group anticipates it will take place in early September.

D. Innovation in Technology and Regulation (H) Working Group

Commissioner Conway reported that the Working Group plans to meet Aug. 29 to hear presentations from the Global Insurance Accelerator (GIA) and InsurTech NY about their programming in support of insurtechs and to discuss what state insurance regulators can do to support the insurtech community. The Working Group is also planning a regulator-only meeting in September to hear from states on how they are using technology to improve regulatory processes.

E. Privacy Protections (H) Working Group

Johnson reported that following the Spring National Meeting, there were several items of note. The Working Group adopted minutes from the four open meetings the Working Group has held since the Spring National Meeting, as well as the minutes from the Spring National Meeting. The Working Group also heard updates from NAIC staff on federal and state privacy legislation efforts. The Working Group also heard comments on specific topics including marketing issues, as well as opt-in and opt-out language related to certain processes discussed in the new *Insurance Consumer Privacy Protections Model Law* (#674). Lastly, the Working Group also discussed asking for additional time to complete the model law. The Working Group will stop taking comments for the time being and will work through the 40 comments received thus far, leading to the exposure of a new draft of the model law. Based on the comments received for the updated model law draft, the Working Group will understand how much additional time would be needed to complete the drafting process.

Welch made a motion, seconded by Executive Deputy Superintendent Finston, to adopt the reports of the Big Data and Artificial Intelligence (H) Working Group (Attachment One); the Cybersecurity (H) Working Group; the E-Commerce (H) Working Group; the Innovation in Technology and Regulation (H) Working Group, including its April 27 minutes (Attachment Two); and the Privacy Protections Working Group (Attachment Three). The motion passed unanimously.

3. Received Comments on the Model Bulletin Exposure Draft

Commissioner Birrane said that the model bulletin draft on the use of algorithms, predictive models and AI was first discussed at the 2022 Fall National Meeting. During that meeting, state insurance regulators discussed that the bulletin would establish a regulatory framework for the use of AI. The regulators chose the approach of a model interpretive bulletin because AI is already subject to regulatory standards and authority. They settled on a principles-based approach with a high-level of standards that would apply generally, focusing on governance. They also acknowledged the importance of validation as part of industry's practices but also recognized practical limitations that sometimes exist. Finally, the regulators settled on placing responsibility for third-party activities on licensees with the expectation that licensees would conduct appropriate due diligence when dealing with third-party data and model vendors.

After deciding on a direction for the bulletin, the regulators convened into four drafting groups with 22 states participating in the drafting process supported by NAIC staff members, including the NAIC's general counsel.

Next, Commissioner Birrane provided a brief summary of the contents of the model bulletin. The bulletin was constructed as regulatory guidance and not as a model law or model regulation, as the regulators decided that existing state laws already apply to the decisions made by insurers using AI systems. The bulletin guides insurers on how to govern their development and use of AI systems that impact consumers, and it also offers guidance on what information and documentation insurers should provide to regulators.

Section 1 of the bulletin gives background and statutory authority in identifying the model laws that provide underlying authority. The regulators recognized that there is not complete uniformity in state laws, so they anticipate that states will adjust the text accordingly. The focus of the bulletin is also on market conduct evaluation and investigation and does not include financial standards for financial examination.

Section 2 identifies definitions for key terms used in the bulletin. The definitions were subject to robust discussion among drafting regulators. Commissioner Birrane specifically invited public comments on the definitions provided in the bulletin.

Section 3 sets the expectation that insurers will establish meaningful governance and risk management policies and procedures and that those policies and procedures will be commensurate with the insurer's AI use.

Section 4 reminds the public that insurers' decisions that are based on AI systems are like any other decisions and are, therefore, subject to review to ensure compliance with the law. The section also provides guidance on the types of information and requests a carrier might expect to see during regulatory reviews of insurer conduct.

With the introduction provided, Commissioner Birrane then opened the floor for discussion, inviting comments from speakers that specifically indicated interest before the meeting in addressing the contents of the model bulletin. Comments were heard from 10 speakers, and each speaker was given three minutes to provide their input.

Peter Kochenburger (Consumer Representative) said that the model bulletin does very little other than describe and expand on what was already expressed in the "NAIC Principles on Artificial Intelligence (AI)" (AI Principles) adopted three years ago. He said the model bulletin missed the opportunity to set guidance and documentation of what insurers need to do when using AI. Kochenburger noted that even for a model bulletin, the language is tentative in areas that it really should not be, such as when encouraging the development of a written automated indicator sharing (AIS) program, which Kochenburger said should be a minimum standard. He also suggested that testing should be required. That way, even in a principles-based approach, regulators can create guidance with teeth to it. Kochenburger also noted that the bulletin reminds insurers that they have to follow state law, but that is already expected as expressed in the AI Principles written three years ago. In some instances, he said the model bulletin represented a step back as well (e.g., when discussing the concept of proxy discrimination against protected classes). Kochenburger said he recognizes the importance of careful wording but after so many years, it is important for the regulators to agree on guidance on unintentional harm.

Dave Snyder (American Property Casualty Insurance Association—APCIA) said that during his years of participation at the NAIC, while there have always been issues and challenges, he did not recall an era where there was so much that was challenging and profoundly disturbing, and as seen with the catastrophe in Hawaii, even tragic. He said the moment calls on regulators and interested parties to work together for the benefit and support of the general public. Regarding the bulletin, Snyder expressed that the overall approach to the model bulletin was correct and that the APCIA appreciated the effort reflected in the draft. He also expressed appreciation for the proportionality and flexibility of the bulletin, as well as the priority that was placed on governance. He added that at first, the bulletin's scope appears to sweep in operations and data that are already adequately regulated and do not need additional regulation. Second, the bulletin's language reflects the current reality of the availability of data and the undesirability of obtaining certain types of data. The APCIA is concerned about any data collection that the public does not want insurers to gather or use. Regarding third-party vendors, the APCIA's smaller insurer members would have some difficulty with these provisions, and that difficulty may extend to larger insurers, as well, in a way that deprives insurers and ultimately the public of beneficial innovation. Fourth, regarding terminology, Snyder emphasized that the legislative standards mentioned in the bulletin should govern the terms used in the bulletin and should not be undermined or modified in favor of any unlegislated standard or terminology. Fifth, the APCIA is concerned about the danger of unnecessary costs. Unless resolved, these issues could impose burdens and ultimately harm, not help, the public. These harms could include increased cost, subpar service, and less technology and information that could help prevent and manage loss. The APCIA asked to continue forward on a bulletin that is appropriately limited in scope, that reflects the realistic status and issues with testing for demographics, helps address third-party vendor regulatory issues without closing off access to the expertise and innovation of other players, adheres in all ways to legislated standards, and results in the most cost-effective bulletin for regulators, insurers, and ultimately, the public.

Dave Sandberg (American Academy of Actuaries—Academy) said that the Academy applauded the bulletin's focus on a framework to document and govern decisions based on AI systems. A focal point of decisions would be essential to assess the depth and breadth of the necessary documentation of governance. Sandberg also drew a comparison of the structure and implementation of governance requirements to the previous effort to implement the Own Risk and Solvency Assessment (ORSA) requirements. He said that the ORSA requirements focus on documenting key risk management principles, measures, and the governance being used by a company. Sandberg further noted that the ORSA requirements were created and drafted over a relatively short period of time. In contrast, he noted that the principles-based reserving requirements were derived over a 20-year period. Therefore, the Academy asked if the framing and implementation requirements of the bulletins were meant to be the same as or different from those used for the ORSA requirements. Sandberg noted that much of the work being done at the Academy and the other actuarial professions is in parallel to this draft bulletin and will be of use to the NAIC and insurance organizations regarding the guardrails and adequate governance needed for AI systems. He said that work at the Academy included content and resources developed by Academy committees, as well as the professional standards for actuarial work that are maintained by the Academy. He stated current applicable standards, include modeling, assumptions setting, and risk classification. Sandberg closed with a reference to the upcoming Center for Insurance Policy and Research (CIPR) educational event during which Dorothy Andrews (Academy) would be sharing further details on projects of the Academy that would be of most interest and applicable to the discussions on the bulletin.

Andrew Pauley (NAMIC) said that NAMIC appreciates the time and effort put into the task of providing a framework and guardrails for insurer use of AI/ML and associated technology systems. Pauley implored the Committee to embrace the many positive aspects of AI/ML that can have important and transformational results for policyholders and consumers. He further stated that NAMIC and its members do not want any legitimate harm to come to consumers or policyholders. NAMIC believes the model bulletin provides a draft framework that can accomplish the Committee's goals while finding common ground with industry and stakeholders. Pauley noted that NAMIC will offer suggestions in the areas of statutory authority to act in these instances; clarification of some of the definitional aspects, such as bias or algorithm; enhanced protections for industry information; risk-based understanding; and needed clarification on some of the principles elucidated in the model bulletin, such as testing and third-party vendor responsibility. He said that NAMIC looks forward to working with the Committee to arrive at solutions that protect and stabilize the insurance marketplace while fostering growth and innovation that benefit all stakeholders.

Brian Bayerle (ACLI) applauded the Committee's leadership for addressing the critical issue of consumer protection. He said that life insurers are increasingly leveraging technology to improve interactions with consumers to make it easier and more convenient to get the financial protections that they need. This includes greater use of technologies that simplify underwriting processes. He said that a regulatory framework designed to eliminate unfair discrimination must be balanced with emerging technologies that help expand the coverage to underserved communities. Bayerle said the model bulletin would allow life insurers to use such technologies to meet consumer demands for an easier, less-intrusive underwriting process while advancing the objective to eliminate unfair discrimination of consumers. However, he said the ACLI has concerns about certain definitions and the imposition of impractical oversight and new contractual obligations on the use of third-party vendors, which will be challenging for smaller to mid-sized companies throughout the country.

Randi Chapman (Blue Cross Blue Shield Association—BCBSA) expressed appreciation for the Committee's work on the model bulletin. She said the BCBSA believes it is important to continue researching and developing best practices and standards for the use of AI tools across all industries. These best practices and standards should focus on emerging risk mitigation that is grounded in the National Institute of Standards and Technology (NIST) *Artificial Intelligence Risk Management Framework*, which includes accountability, security and safety, privacy and confidentiality, transparency and explainability, reliability, fairness, and bias mitigation. The BCBSA supports the development of a risk-based approach that measures the need for appropriate protections without stifling innovation, and it encourages the NAIC to coordinate with federal regulatory partners, like NIST, to promote consistency in AI governance best practices. The BCBSA believes that consistent and uniform standards that address algorithm documentation, testing, and auditing, as well as stakeholder education, will foster greater trust and accountability in AI tools.

Michael DeLong (Consumer Representative), on behalf of the Consumer Federation of America (CFA), said consumer groups have long been concerned about protected class unfair discrimination generated by insurer use of data that are racially biased, which indirectly cause unfair discrimination on the basis of race. DeLong added that with insurers' explosive growth in using new sources and the types and volumes of data and AI, state insurance regulators acknowledged the increased potential for racially biased data and algorithms to produce protected class unfair discrimination in 2020 with the adoption of the AI Principles. Shortly after the adoption of the AI Principles, the NAIC created the Special (EX) Committee on Race and Insurance, which is charged with determining if current practices exist in the insurance sector that potentially disadvantage minorities. DeLong said that while the NAIC has done much on diversity, equity, and inclusion (DE&I) among insurers and regulators, structural racism in insurance has not been addressed. He further stated that the model bulletin is not principles-based, but a prescriptive governance approach that does not expand on the AI Principles nor provide specific guidance, principles-based or otherwise, to NAIC committees, working groups, insurers, or regulators on how to implement the AI Principles. DeLong noted that it fails to provide essential definitions, does not define proxy discrimination, fails to address structural racism in insurance, and incorrectly tells insurers that testing for protected class bias may not be feasible.

Birny Birnbaum (Center for Economic Justice—CEJ) said that AI governance, risk management procedures, and documentation are necessary and important but not sufficient. Birnbaum stated the emphasis should be placed on testing consumer outcomes for fair and unfair discrimination during all phases of the insurance life cycle and in both model development and post-deployment. Birnbaum added that regulatory guidance is needed to generate this testing, including proxy discrimination defining, to establish at least one uniform testing methodology, reporting of testing results by insurers, and to establish thresholds for what constitutes proxy discrimination. Birnbaum said that for some issues such as for cybersecurity, it is necessary to rely on good hygiene or process guidance to try to prevent bad outcomes because there are not enough outcomes against which to apply predictive analytics. Insurers have and regulators can obtain the data and ability to ensure good market outcomes and compliance through testing of these outcomes for fair and unfair discrimination. Testing should be the central feature of governance. Meaningful guidance regarding the fairness prong of the AI Principles must include insurer data testing guidance. Testing for racial bias has been done for housing, employment, credit, and even insurance for five decades. There are well-accepted methods for such testing so that regulators do not have to invent their own methodology. Birnbaum gave an example of what would happen if a governance-only approach to financial solvency was enacted, but it would not make sense with metrics, such as risk-based capital (RBC), giving regulators the ability to quickly review and compare hundreds of insurers and their relative financial

© 2023 National Association of Insurance Commissioners

condition. He added that the same logic behind a standard methodology and standard metrics for RBC should apply to establishing standard metrics and testing methodology for insurer's use of AI.

Jim Hodges (National Alliance of Life Companies—NALC) said that the principal-based approach is the correct approach. However, he stated that the NALC wanted to raise several issues, with the first being the uneven negotiating power of small versus large companies. Vendors in smaller companies may not enjoy the same level of cooperation or abilities to modify terms and conditions that the larger companies have. The second issue involves better defining specific terms around AI to discern between newer technologies versus algorithms that have been around for decades. Hodges also noted that other federal and state regulators are wrestling with the same issues and encouraged regulators to collaborate to provide consistent definitions to spur innovation and ensure a more consistent approach for consumers, insurers, and regulators. Hodges stated the importance of engaging with technology companies to share the sensitivity points of regulators and to try to have those issues addressed. He said an ongoing dialogue will lead to better products that address regulatory concerns and regulatory mandates. Hodges noted the bulletin also references the federal Unfair Trade Practices Act and is concerned that utilization of new AI tools may be deemed appropriate in one state and an unfair trade practice in another, which will discourage the use of innovative tools. Where possible, companies and regulators should work together to advance the use of innovative tools on a consistent and uniform basis. The NALC also believes that pilot initiatives around new regulatory approaches should be undertaken to test both effectiveness and fairness.

J.P. Wieske (American InsurTech Council—AITC) expressed appreciation for the time regulators have taken to work with industry representatives on the continued development of the model bulletin. Wieske further said the AITC appreciates that the bulletin requires insurers to have the same standard across anything they use fundamentally in their insurance products and gives regulatory authority that makes sense, is consistent, and is time-tested. Wieske said the AITC acknowledged that many concerns have been raised on what AI is and raised that the definitions in the model bulletin may need to be revised. He also expressed that AI is simply another tool available to insurers that should be held to the same standards that insurers have to meet today. Wieske said that while he understands that there are concerns on the use of AI, those concerns are likely reflective of already existing concerns in the current marketplace. The AITC would like the NAIC to consider the process that exists in market conduct, which is more generally around self-audit and comprehensive self-audit, and is not mentioned in this bulletin. Wieske encouraged the NAIC to work with large, medium, and small companies privately to better understand how AI is being used in insurance.

Commissioner Birrane then opened the floor for discussion from Committee membership, other regulators, or interested parties.

Commissioner Humphreys posed that a general question be issued to companies in order to incorporate feedback in written comments about the oversight of third-party groups regarding compliance with non-discrimination laws. He said he has heard from companies that do feel they have the power to require cooperation with insurance departments but is unsure if that would be true for companies of all sizes. Commissioner Humphreys has also heard from smaller companies that feel they have little to no power to negotiate such terms. He drew a comparison to pharmacy benefit managers and wondered about the possibility of licensing service providers similar to rating organizations where departments have to work with the service providers to get into compliance. Commissioner Humphreys asked for feedback on third-party oversight that would give companies comfort in knowing that the service providers are not discriminating.

Chou asked the Academy to elaborate on how effective ORSA is given that many companies treat the filing as a compliance exercise.

Sandberg responded to Chou that the value of ORSA is that it lays a foundation for productive conversations. Sandberg continued by noting that AI is emerging, and the ability to have a set of metrics will be a long process and will be a good foundation for having further productive conversations. He added the ORSA filings allow companies to engage with regulators about their controls and emerging risks. He drew a parallel to AI-related discussions, noting the process to develop a set of metrics that remain unchanged and are codified will require a foundation to be laid.

Commissioner Conway added to Commissioner Humphrey's commentary said on the third-party aspect of the bulletin. He noted that if the regulators are going to have an outcome-focused testing methodology, then third parties will necessarily need to be involved. Conway noted it is important for companies to address this testing, and if there is a problem with third-party agreements, he questioned how industries will respond if there is a problem with outcome-testing.

Commissioner Birrane then opened the floor to any others who did not sign up to speak ahead of the meeting. Brendan Bridgeland (Center for Insurance Research—CIR) pointed out one sentence in the bulletin that he found troubling, which he quoted: "Current limitations on the availability of reliable demographic data on consumers make it challenging for insurers and regulators to directly test these systems to determine whether the decisions made meet all applicable legal standards." Bridgeland stated this sentence should not be in the bulletin, as it undermines the power of regulatory authority, implying that regulators will not be able to deal with this in the future.

Director Wing-Heier said that the bulletin is a good working document. She said she appreciated the hours spent on it and acknowledged the bulletin has been a significant project and represents a good start.

Commissioner Birrane concluded by stating that when the Committee receives all the written public comments, the Working Group will meet in regulator-to-regulator session, and then it will present a second draft of the model bulletin at the end of September.

Having no further business, the Innovation, Cybersecurity, and Technology (H) Committee adjourned.

SharePoint/NAIC Support Staff Hub/Member Meetings/H Cmte/2023_Summer/H-Minutes/H-Cmte-Minutes081323 v4docx

Draft: 8/28/23

Big Data and Artificial Intelligence (H) Working Group
Seattle, Washington
August 13, 2023

The Big Data and Artificial Intelligence (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Seattle, WA, Aug. 13, 2023. The following Working Group members participated: Elizabeth Kelleher Dwyer, Chair (RI); Amy L. Beard, Co-Vice Chair, represented by Victoria Hastings and Alex Peck (IN); Doug Ommen, Co-Vice Chair (IA); Adrienne A. Harris, Co-Vice Chair, represented by John Finston (NY); Kevin Gaffney, Co-Vice Chair (VT); Mark Fowler (AL); Barbara D. Richardson (AZ); Michael Conway, Peg Brown, and Debra Judy (CO); Andrew N. Mais, George Bradner, and Wanchin Chou (CT); Susan Jennette (DE); Rebecca Smith (FL); Shannon Hohl (ID); Erica Weyhenmeyer (IL); Chuck Myers (LA); Rachel M. Davison (MA); Kathleen A. Birrane (MD); Timothy N. Schott (ME); Karen Dennis (MI); Phil Vigliaturo (MN); Cynthia Amann (MO); Colton Schulz (ND); Eric Dunning (NE); Christian Citarella (NH); Matt Walsh (OH); Teresa Green (OK); Alex Cheng (OR); Shannen Logue, Katie Merritt, and Michael McKenney (PA); Ryan Basnett (SC); Travis Jordan (SD); Stephanie Cope (TN); Mark Worman (TX); Scott A. White (VA); Bryon Welch (WA); Rachel Cissne Carabell (WI); and Erin K. Hunter (WV). Also participating were: John F. King (GA); and Matt Gendron (RI).

1. Adopted its Spring National Meeting Minutes

Commissioner Ommen made a motion, seconded by Commissioner Gaffney, to adopt the Working Group's March 22 minutes (*see NAIC Proceedings – Spring 2023, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Two).* The motion passed unanimously.

2. Received an Update on the AI/ ML Surveys

Commissioner Gaffney said the Artificial Intelligence (AI)/Machine Learning (ML) surveys are being conducted to accomplish three goals: 1) gain a better understanding of the insurance industry's use and governance of big data and AI/ML; 2) seek information that could aid in the development of guidance or potential regulatory framework to support the insurance industry's use of big data and AI/ML; and 3) inform state insurance regulators as to the current and planned business practices of companies. Commissioner Gaffney said the public report of the Private Passenger Automobile (PPA) AI/ML survey was distributed at the 2022 Fall National Meeting and is posted on the NAIC website under the Big Data and Artificial Intelligence (H) Working Gorup.

Commissioner Gaffney said the public report of the Home AI/ML survey has been issued. The Home Insurance survey was conducted under the examination authority of 10 states (Connecticut, Illinois, Iowa, Louisiana, Nevada, North Dakota, Pennsylvania, Rhode Island, Vermont, and Wisconsin) and was issued to insurers having at least $50 million in national homeowners written premium in 2020. Just like the PPA survey, the requesting states agreed the collected data will not be used to evaluate or determine a company's compliance with applicable laws and regulations and that all company-specific information will be kept confidential under state examination authority.

Commissioner Gaffney said the survey was focused on the use of AI models, which include ML, but it was specifically limited to exclude the use of more traditional generalized linear models (GLMs) in the areas of claims, fraud identification, marketing, rating, underwriting, and loss prevention. He said the survey also asked about data elements used by operational area, how consumers are notified of the use of data and their ability to request a correction to data being used, how governance is documented in the company's governance framework, and the names of third-party vendors providing data and/or external models.

Out of the 194 companies completing the survey, Commissioner Gaffney said 136 companies (or about 70%) use, plan to use, or plan to explore using AI in their operations. This is not quite as high as the 88% of the responses received from the PPA survey, which may be due to less usage of AI/ML claims models in homeowners insurance. Among insurer operations areas, Commissioner Gaffney said the percentage of companies using AI models in homeowners insurance were: 1) claims, 54%; 2) underwriting and marketing, both at 47%; 3) fraud detection, 42%; 4) rating, 35%; and 5) loss prevention, 14%. He said the main reasons reported for not using, not planning to use, and not exploring the use of AI for home insurance were: "no compelling business reason"; "waiting for regulatory guidance"; and "lack of resources and expertise." In the claims function, the home insurers reported using AI mostly for subrogation, claims triage, and evaluating images of loss.

Commissioner Gaffney said home and PPA insurers use claims models to analyze images of loss. Home insurers also use claims models to determine subrogation and for claims triage. He said home insurers do not use claims models to make claim assignment decisions or to determine settlement amounts as much as reported in the PPA survey. AI/ML claims models for both home and PPA were generally developed in-house except those used to evaluate images, which tend to be developed externally.

For fraud identification, Commissioner Gaffney said both PPA and home insurers reported using AI mainly to refer claims for further investigation, with some using AI to detect organized crime rings. Some home insurers also reported using social media for fraud identification. For both home and PPA, fraud models were mixed between internally and externally developed models.

For marketing, Commissioner Gaffney said both home and PPA insurers are generally using AI for targeted online advertising. Generally, the marketing models used in both PPA and home were reported about equally developed in-house and purchased from a third party.

For rating and underwriting, Commissioner Gaffney said there was less usage of advanced AI/ML models reported, mainly reflecting the transparency requirements by state insurance regulators, where more traditional GLMs provide this transparency. Almost all rating and underwriting models were developed in-house. Home insurers reported that most models used in underwriting were for automated or augmented denial decisions and for verification of policy characteristics.

For loss prevention, Commissioner Gaffney said 28 home insurers reported using AI mainly for guidance on loss control inspections, but only three PPA insurers reported using AI for loss prevention.

Commissioner Gafney said a variety of typical data elements are being used in home and PPA insurance depending on the model purpose and that insurers are also looking at a lot of geo-demographic data externally sourced. For marketing, insurers are looking at a lot more types of data to identify prospects than would be allowed for use in ratemaking or underwriting, such as data on occupation, education, personal finance information, and income.

When asked about information provided to policyholders about how their data is being used and opportunities to correct their data, Commissioner Gaffney said there was a low response rate from insurers reporting they do more than what is required by existing statutes and regulations.

Regarding insurers' documented governance practices as aligning with the NAIC Principles on AI, Commissioner Gaffney said roughly half of insurers reported they have a documented governance program that considers the elements of the NAIC Principles on AI.

Commissioner Gaffney said potential next steps include exploring insurers' AI model usage and the level of decision-making, evaluating the regulatory framework for the use of third-party models, and determining whether additional white papers on best practices on subjects related to AI/ML would be useful. There were no additional comments or questions from the Working Group members or interested parties.

3. Heard a Presentation from Deloitte on Generative AI

Superintendent Dwyer said the next agenda item is to hear a presentation on generative AI from David Sherwood (Deloitte) and Casey Kacirek (Deloitte). Before hearing the presentation from Sherwood and Kacirek, Superintendent Dwyer said NAIC staff asked ChatGPT, which is an example of generative AI, to explain what Generative AI is. The following, edited for brevity, is what ChatGPT produced:

Generative AI refers to a category of artificial intelligence techniques that focus on creating or generating new content, data, or information. These techniques are particularly useful in tasks where creativity, imagination, and pattern recognition are required. When explaining generative AI to state insurance regulators, you can use the following approach: Generative AI involves training a computer program to generate content that is similar to, but not identical to, existing data. It's like teaching a computer to come up with its own versions of things it has seen before. Generative AI models are trained on large datasets to understand the patterns, styles, and structures present in the data. These models then use this knowledge to create new content that fits within the learned patterns. For example, a generative AI model trained on insurance claim data can generate new, plausible insurance claims based on the patterns it has learned.

Sherwood said AI has been around a long time, and credit card companies use it to detect fraud. Sherwood said generative AI is a hot topic of discussion. Sherwood said Deloitte has a concept called trustworthy AI, and organizations need to think about what controls are in place for AI conducting tasks.

Kacirek said AI is technology striving to mimic human behavior. This encompasses several technologies that work together, including ML, natural language processing, predictive analytics, and speech processing. In terms of the evolution of AI, Kacirek said generative AI is creating content based on human prompts by leveraging robust data sources that are either internally or externally available. Natural language processing (NLP) is another emerging technology, which is the ability to understand text and spoken words. Kacirek said Alexa and Siri are based on the ability to understand human language. Computer vision is another technology that has been in existence and is essentially image recognition, such as facial recognition to unlock a phone. She said Netflix and Hulu use near real-time interfacing to provide consumers recommendations based on the analysis of real-time data on how a consumer is selecting a show. Kacirek said these four technologies are driving the emerging capabilities of AI.

Kacirek said a business could have an initial draft of code written through generative AI and have that draft be the basis for a human coder to review and leverage. Generative AI can also be used for marketing and creative design work. Generative AI can produce a wide range of outputs depending on the specific application and type of data that is needed. Some common output types include text, video, code, image, and audio. Sherwood said generative AI is being used in insurance to create text. For example, draft job descriptions or consumer communications on certain types of claims might be prepared using generative AI. Insurers can then use a human in the loop to review these outputs. For call centers, insurers might use audio generative AI where a human is answering calls with generative AI listening and providing suggested prompts to the types of questions being asked.

Kacirek said the use of external data and third-party data requires monitoring and controls to be in place and that that a human should be responsible for the output. Sherwood said it is unlikely that insurers will be developing their own generative AI systems because there are already leaders in this field. Sherwood said it is important to understand how insurers integrate this technology with their existing technology and how both internal and external data might be leveraged.

Kacirek said there are potential risks with using generative AI, including bias since models are leveraging robust data sets. She said data may have unintentional bias, such as demographic data or protected class data. Because of this, there is a need to monitor for potential bias, and having some level of human supervision during the training of a model is one way to address bias risk. Periodic monitoring is also needed to assure the model continues to perform as anticipated. Kacirek said companies should consider whether the use of a model output is ethical to use. She said another risk is hallucination, which occurs when a model produces an output that sounds plausible but is factually incorrect. Kacirek said this may occur because of poor data quality. Sherwood said generative AI is mimicking human behavior and that risk and control are important because AI works at a higher velocity than humans.

Kacirek reviewed Deloitte's Trustworthy AI framework is intended to provide a framework to address the risks associated with the use of AI. She said the framework is rooted in the National Institute of Standards and Technology (NIST) AI framework. Kacirek said the Deloitte framework includes the following concepts:

- **Fair and impartial**: This involves assessing whether systems include internal and external checks to assure equitable application across all participants and that there is no bias towards certain groups or protected classes. Companies can assess this risk by conducting fairness testing and reviewing whether models are providing any discriminatory outcomes.
- **Transparent and explainable**: Participants can understand how their data is being used and how AI systems make decisions. This means questioning whether algorithms and attributes are open to inspection and whether the outcomes are explainable.
- **Responsible and accountable**: This involves making sure policies are in place to determine who is held ultimately responsible for the output of AI system decisions.
- **Robust and reliable**: This focuses on having the appropriate, minimum requirements or checks for reliability and consistency of an AI model prior to deployment. This also involves ongoing checks after deployment to make sure the model performs as intended.
- **Privacy**: This involves elevating consumer privacy to make sure customer data is not used beyond its intended and stated use.
- **Safe and secure**: This involves elevating safety and security to assure AI systems are protected from risks, including cyber risk.

Kacirek said approximately 50% of organizations have adopted some framework for governing the use of AI. She said companies have an opportunity to leverage existing risk management processes, which have roles and responsibilities, policies and procedures, processes and technology, and aspects of cross-functional compliance. Sherwood said a good example of leveraging existing model risk management is for a company to review the list of models being used and to identify which models are using AI. This might lead to further scrutiny about what data is being used and the third parties being used.

Kacriek said building a trustworthy AI environment involves the concept of establishing three lines of defense. The first line of defense is for the business users to own the model and its outputs. The second line of defense is for a company to establish governance and compliance requirements. The third line of defense is for a company to have an independent review of models. Kacirek said business owners should be performing testing and validation of a model before it is deployed, and there should then be validation, monitoring, and controls in place. She said it is important for companies to understand how quickly they can respond to unintended outcomes of an AI model.

Sherwood said companies should look at the use of AI throughout the value chain and upskill staff in the use of AI. He said there are tasks that may be automated to enhance consumer outcomes or eliminate costs for the company. Sherwood provided an example of the use of accelerated underwriting, chat features of call centers, and the use of AI in claims settlement and fraud detection.

Superintendent Dwyer said it is important for insurance companies to be able to explain how their AI models work. Commissioner Ommen said transparency is an important consumer protection. For example, insurance companies may not be able to adequately explain to a consumer why a claim is being delayed or denied. Sherwood said a model should be generating an outcome, which is reviewed by a human, who then communicates the outcome to the consumer.

Commissioner Birrane said insurers should be able to explain what is causing an adverse decision or outcome for a consumer. Kacirek said a model will evolve over time and that a company should be accessing decisions that are considered outliers. The company can then assess the frequency of these outcomes and use these outcomes for possible training of the model within established guardrails.

Commissioner Gaffney asked how to minimize the risk of overreliance on data. Kacirek said there should be controls to monitor the completeness and accuracy of data prior to its use and ongoing monitoring. Companies should also make sure the data is fit for the intended purpose of the model. In response to Commissioner Gaffney's question about upskilling of state insurance regulators, Sherwood said upskilling should be completed in layers with foundational education provided to a broader set of staff and then more specific training provided to staff based upon their specific role. Sherwood said state insurance regulators should understand control environments and engage with industry to understand challenges. In response to Commissioner Gaffney's question about how AI could be used to reach underserved markets, Sherwood said automation of functions may help lower costs and could potentially lead to more affordable and available insurance.

Having no further business, the Big Data and Artificial Intelligence (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Committees/H CMTE/2023_Summer/WG-BDAI/BDAI Minutes 081323.docx

Draft: 6/26/23

Innovation in Technology and Regulation (H) Working Group
Virtual Meeting
April 27, 2023

The Innovation in Technology and Regulation (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met April 27, 2023. The following Working Group members participated: Jason Lapham, Chair (CO); Dana Popish Severinghaus and C.J. Metcalf, Co-Vice Chairs (IL); Matt Walsh, Co-Vice Chair (OH); Erick Wright (AL); Letty Hardee (AR); Lucy Jabourian (CA); George Bradner (CT); Dana Sheppard (DC); Tim Li (DE); Gordon I. Ito (HI); Jared Kirby (IA); Weston Trexler (ID); Shannon Lloyd (KS); Abigail Gall (KY); Rachel M. Davison (MA); Kory Boone (MD); Sandra Darby (ME); Chad Arnold (MI); Cynthia Amann (MO); Ryan Blakeney (MS); Chris Aufenthie and Colton Schulz (ND); Cassie Soucy (OR); Shannen Logue (PA); Joe McElrath (TX); Melissa Gerachis (VA); Eric Slavich (WA); Jennifer Stegall and Timothy Cornelius (WI); and Juanita Wimmer (WV).

1. Discussed an Overview of its 2023 Work Plan

Lapham said the Working Group's 2023 work plan was submitted to the Innovation, Cybersecurity, and Technology (H) Committee leadership. At the Spring National Meeting, Commissioner Michael Conway (CO) gave an overview of the work plan during the Committee's meeting. He said the Working Group plans to develop a SupTech Forum to allow state insurance regulators to share insights on current innovations and technologies they use in their respective states. He said the Working Group is also looking to develop an Insurtech Forum that will allow state insurance regulators to have one-on-one discussions with insurers and third-party insurtechs that work with insurers about the types of technologies and innovations those insurers and third parties are using, as well as the regulatory barriers and opportunities that exist around those technologies. He said the Working Group will monitor industry developments and create insurtech training for state insurance regulators. As issues arise, the Working Group will pass along referrals to the appropriate NAIC working group or committee.

2. Discussed the Development of a SupTech Forum

Lapham said the idea of a SupTech Forum is for a regulator-to-regulator webinar that would be a forum for states to present on supervisory technologies they are using, which would be beneficial for other state insurance regulators to hear about. He said the point of the webinar is to foster innovative thinking on how state insurance regulators do their jobs. He said one example of supervisory technology is the North Dakota project using blockchain technology to collect uninsured motorist data.

Brander said he would volunteer to present a webinar on Connecticut's use of artificial intelligence (AI) and machine learning (ML) to review files.

Boone said Maryland has many projects it is working on. He said examples include digitizing portable document formats (PDF files) to make it easier for people to fill out forms on their tablets or smartphones using a ticketing system to track complaints and upgrading enterprise accounting software.

Lapham said the goal is to display various supervisory technologies because not all technologies will work in every state. He said small technology upgrades are just as important to showcase as large, innovative projects.

3. Discussed the Development of an Insurtech Forum

Lapham said Working Group leadership and NAIC staff drafted an outline of an Insurtech Forum program to be held at the 2023 NAIC Insurance Summit. He said the Working Group is looking for volunteers to assist with designing and participating in the program.

Lapham said the forum's objective is to facilitate conversations between state insurance regulators, insurers, insurtechs, and interested parties about the types of innovations and technologies available to insurers and insurtechs and the potential regulatory barriers and opportunities. He said the goal is to invite four to six insurtech companies to engage in conversations with the participants in a round-robin style setting. He said it would be helpful to hear from state insurance regulators and interested parties that have participated in similar events to finetune the forum before the launch at the Insurance Summit.

Logue said she would support this effort. She said Pennsylvania created a pipeline that facilitates these conversations with insurers and insurtechs to discuss their innovative technologies with state insurance regulators. She said a forum like this would be a good opportunity to have state insurance regulators from multiple states weighing in on the conversations.

Amman suggested contacting the Insurance Regulatory Examiners Society (IRES) and the Society of Financial Examiners (SOFE) to ask about possible presenters or volunteers for both the SupTech Forum and Insurtech Forum initiatives.

Miguel Romero (NAIC) said the perspective from interested parties would benefit the program's design and implementation.

4. Heard a Presentation from the Aite-Novarica Group on ChatGPT

John Keddy (Aite-Novarica Group) said ChatGPT and other emerging technologies are the hottest topics across all insurance industry sectors. He said the Aite-Novarica Group surveyed the industry and collected data on various technologies. He said in the property/casualty (P/C) industry, interest lies in cloud computing, low-code and no-code technologies, and AI. He said there is also a developing interest in unstructured data. He said the life, annuities, and benefits industry has shown similar interest, with an even higher deployment rate of these technologies driven by larger carriers. He said chatbots have a high deployment rate across the industry, but that technology differs from the technology behind ChatGPT.

Keddy said large insurers especially are taking advantage of data lakes to transform enterprise data management. He said insurers of all types recognize the value of "big data" sources. He said interest in blockchain technology remains more modest.

Keddy said P/C insurers have invested heavily in ML and unstructured text capabilities. He said data is used to drive the training of algorithms in AI. He said the life, annuities, and benefits industry has a higher deployment rate of unstructured text capabilities and voice recognition technology.

Keddy said the survey results show that sustained investment in data, plus broad interest in AI, investment in cloud technology, and fervor around technologies like ChatGPT means now is the time for engagement in AI topics.

Keddy said when discussing AI, it is best first to define the technology, as there are many different technologies under the AI umbrella. He said the trajectory of the AI conversation has rapidly increased in 2023 due to the excitement around ChatGPT. He said ChatGPT is just one technology under the natural language processing part of AI. He said it is best for companies to not only focus on ChatGPT but to look holistically at AI and its uses within the company.

Keddy said outside of the insurance industry, AI has already arrived. He said examples include home security, medical scanning for tumors or diseases, and cybersecurity.

Keddy said his perspective on AI technology is that it should remove abstractions and work within reality, and AI decisions must be explainable and compared to human decisions.

Keddy said technologies and data scientists testing out new models and approaches have more risks. He said automated ML allows people who do not understand the technologies, statistics, or data to create new models, which is a high-risk activity.

Keddy said the takeaways of this discussion include the following: 1) due to sustained investment and recent fervor, now is the time for a conversation on emerging technologies; 2) ChatGPT is an incredibly powerful tool, but the industry should focus on the larger conversation of AI; and 3) the force must be respected, but fundamental principles must not be abandoned.

Lapham said the Working Group will continue to monitor these fast-moving emerging technologies and consider the possibility of developing state insurance regulator training on these technologies.

Having no further business, the Innovation in Technology and Regulation (H) Working Group adjourned.

SharePoint/NAIC Support Staff Hub/Member Meetings/H CMTE/ Summer 2023/WG-ITR/Inn In Tech and Reg WG Minutes Final 042723.docx

© 2023 National Association of Insurance Commissioners

Draft: 8/30/23

Privacy Protections (H) Working Group
Seattle, Washington
August 13, 2023

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met in Seattle, WA, Aug. 13, 2023. The following Working Group members participated: Katie Johnson, Chair (VA); Cynthia Amann, Vice Chair (MO); Lori K. Wing-Heier (AK); Catherine O'Neil (AZ); Damon Diederich (CA); George Bradner (CT); Erica Weyhenmeyer (IL); LeAnn Crow (KS); Ron Kreiter (KY); Van Dorsey (MD); Robert Wake and Sandra Darby (ME); Jeff Hayden (MI); T.J. Patton (MN); Santana Edison represented by Colton Schulz (ND); Martin Swanson (NE); Teresa Green (OK); Raven Collins (OR); Gary Jones (PA); Patrick Smock (RI); Frank Marnell (SD); Todd Dixon (WA); Rachel Cissne Carabell and Timothy Cornelius (WI). Also participating were: Sarah Bailey and Heather Carpenter (AK); Peg Brown (CO); Doug Ommen (IA); Victoria Hastings (IN); Jamie Sexton (MD); Eric Dunning (NE); Judith L. French (OH); Matthew Tarpley (TX); and Don Beatty (VA).

1. Heard Opening Remarks

Johnson said the Working Group has what looks like a simple agenda, but it has important discussions ahead of it. She said she and the Working Group would like to thank everyone who has been and continues to be an important part of this transparent, collegial, and collaborative process, especially those who spent considerable time, money, and input for two full days—four days including travel time—to dig into seven important issues with the model.

Johnson said she would like to give an update on the Working Group's activities to ensure all stakeholders are on the same page going forward. She said the 60-day comment period for the first draft of the new *Insurance Consumer Privacy Protections Model Law* (#674) ended April 3.

Johnson said the drafting group met with companies privately to discuss current consumer data practices on May 9, May 4, April 28, April 27, April 20, April 13, April 12, April 11, April 6, and April 5.

Johnson said the Working Group met July 25, June 5–6 at an in-person meeting in Kansas City, MO; May 16; May 2; April 18; and at the Spring National Meeting to discuss comments received and collaborate on workable language. She said the interim meeting sessions were working sessions focused on the drafting of model language. She said the 112 in-person attendees—29 state insurance regulators, including one commissioner; three NAIC consumer representatives; 68 industry representatives; and 12 NAIC staff members—were asked to be prepared to consider new language and offer their pros and cons. She said participants were asked to keep their comments specific to the topic under discussion. She said topics already discussed in open meetings were not revisited during this meeting.

Johnson said a drafting group met Aug. 9, July 20, July 10, July 7, June 30, June 29, June 26, June 23, June 2, May 17, May 12, and May 5 in regulator-to-regulator session.

Johnson said because Version 1.2 of the new Model #674 was based on changes discussed at the interim meeting, the Working Group exposed it July 11 for a public comment period ending July 28. She said the drafting group privately continued its meetings with industry trades and companies to discuss current consumer data practices Aug. 9, meetings with two different companies on Aug. 3, Aug. 2, and July 28.

© 2023 National Association of Insurance Commissioners

Johnson said the Working Group sent interested parties an invitation that it would continue scheduling private calls with trades, companies, and other interested parties. She said the Working Group also notified interested parties that so many comment letters had been received since the interim meeting that the Working Group has been unable to post them all prior to the Summer National Meeting. She said the Working Group will continue posting comments to the website after the national meeting. She said due to the sheer volume of comments and the number of one-on-one calls requested, the Working Group has determined that more time is needed to engage the public and continue drafting the model.

2. Adopted its July 25, June 5–6, May 16, May 2, April 18, and Spring National Meeting Minutes

Johnson said the Working Group met July 25, June 5–6, May 16, May 2, and April 18. During its meetings, the Working Group took the following action:

A. Discussed comments received and collaborated on workable language regarding the following seven topics:
   i. Third-party service providers, including the definition of third-party service providers, third-party service providers not related to an insurance transaction but that have access to consumers' personal information, and contracts with third-party service providers.
   ii. Definitions of insurance transactions and additional permitted transactions.
   iii. Marketing, including marketing insurance products to consumers using consumers' personal information, marketing other products to consumers using consumers' personal information, and affiliate marketing.
   iv. Joint marketing agreements (JMAs), JMAs with affiliates, and JMAs with non-affiliated third parties.
   v. Opt-in versus opt-out consent to marketing and the difference between marketing insurance and non-insurance products.
   vi. Notice of Consumer Privacy Practices – Contents.
   vii. Notice of Consumer Privacy Protections – Frequency and Methodology of Delivery.
B. Drafted Model #674 language. In-person attendees were asked to be prepared to consider the new language and offer pros and cons. Participants were asked to keep their comments specific to the topic under discussion. Topics already discussed in open meetings were not revisited during this meeting.
C. Exposed Version 1.2 of the new Model #674 on July 11 because it was based on changes discussed at an interim meeting, with a public comment period ending July 28. The drafting group continued its meetings with industry trade companies privately Aug. 9, Aug. 3, Aug. 2, and July 28 to discuss current consumer data practices.
D. Notified interested parties that so many comment letters have been received since the interim meeting that the Working Group has been unable to post them all prior to the Summer National Meeting. The Working Group will continue posting comments to the website after the national meeting. Due to the sheer volume of comments and the number of one-on-one calls requested, the Working Group has determined that more time is needed to engage the public and continue drafting Model #674.
E. Discussed comments received and engaged the public to continue drafting Model #674.

The Working Group also met Aug. 12 in regulator-to-regulator session, pursuant to paragraph 4 (internal or administrative matters of the NAIC or any NAIC member) of the NAIC Policy Statement on Open Meetings.

Amann made a motion, seconded by Diederich, to adopt the Working Group's July 26 (Attachment Three-A), June 5–6 (Attachment Three-B), May 16 (Attachment Three-C), May 2 (Attachment Three-D), April 18 (Attachment Three-E), and March 22 (*see NAIC Proceedings – Spring 2023, Innovation, Cybersecurity, and Technology (H) Committee, Attachment Three*) minutes. The motion passed unanimously.

3. Heard Updates from NAIC Staff on State and Federal Privacy Legislation

Jennifer Neuerburg (NAIC) said in the continuing absence of congressional action on a comprehensive U.S. federal privacy law, many states have enacted state data privacy laws or are considering legislative action. She said on June 30, the Delaware legislature passed the Delaware Personal Data Privacy Act (HB 154), and the bill is ready for governor consideration. She said assuming that the bill becomes law, Delaware will become the 12th state—the seventh this year—to pass a consumer data privacy law. The other states that have passed bills this year are Indiana, Iowa, Montana, Oregon, Tennessee, and Texas. Neuerburg said at least 16 additional states have introduced data privacy bills during the current legislative cycle that are either comprehensive in nature or address a range of data privacy issues, and if anyone wants to read more about these bills, there are charts tracking state legislation on the Working Group's web page.

Shana Oppenheim (NAIC) said the privacy legal and regulatory landscape is changing quickly in the U.S., particularly for financial institutions, which hold significant volumes of consumer data. She said at the federal level last year, the U.S. Congress (Congress) made significant bipartisan progress on comprehensive federal privacy legislation, advancing the proposed federal American Data Privacy and Protection Act (ADPPA), which passed out of the U.S. House of Representatives (House) Committee on Energy and Commerce with a 53-2 vote and almost made it to a House floor vote. Earlier this year, she said the House Committee on Energy and Commerce's new Subcommittee on Innovation, Data, and Commerce held a hearing in March titled "Promoting United States Innovation and Individual Liberty Through a National Standard for Data Privacy." Additionally, she said House Financial Services Committee Chair, Patrick McHenry's, financial data privacy bill, the Data Privacy Act of 2023 (H.R. 1165), passed out of the Committee along party lines in February. She said it would: 1) revamp existing financial privacy protections for consumers under the federal Gramm-Leach-Bliley Act (GLBA); and 2) create a preemptive ceiling and floor to create a uniform federal standard. She said the current bill allows for enforcement by functional regulators, provides a new deletion right for consumers, and allows consumers to stop collecting and disclosing their data, among other provisions. She said Representative Maxine Waters (D-CA) and the Democrats have been critical of any preemption because it would hinder the states' ability to act as a laboratory for innovation while establishing a weak federal standard. She said although there seemed to be some legislative momentum earlier this year, nothing has yet come of it. She said more limited/focused data privacy actions seem more likely. For example: 1) the House Judiciary Committee also approved a bill in July that would ban law enforcement agencies from buying people's sensitive information from data brokers—the Fourth Amendment Is Not For Sale Act; and 2) for the second consecutive year, the U.S. Senate (Senate) has approved two children's online privacy measures—the Kids Online Safety Act (KOSA)—for floor consideration just before departing for the month-long August recess. Oppenheim said KOSA is focused on social media companies and children's data. She said U.S. state insurance regulators are also drafting several regulations that may be pertinent: 1) the Consumer Financial Protection Bureau (CFPB) is in the process of issuing a rule for the long-awaited implementation of Section 1033 of the federal Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), which would require that consumers be able to access their financial data. She said the rule may specifically affect checking, savings, and credit card accounts. It is expected later this year with a final rule slated for 2024; 2) the CFPB also launched an inquiry into data brokers under the federal Fair Credit Reporting Act (FCRA), and it is attempting to understand the "full scope and breadth of data brokers and their business practices, their impact on the daily lives of consumers, and whether they are all playing by the same rules." She said the Federal Trade

Commission (FTC) is also investigating commercial surveillance industries, which it defines as collecting, analyzing, and profiting from information about people. She said the term encompasses the collection, aggregation, analysis, retention, transfer, or monetization of consumer data. She also said in an advanced notice of proposed rulemaking in August 2022, the FTC posed 95 questions about consumer harm, data security, and related topics to commercial surveillance companies.

4. Discussed an Extension to Develop the New Model #674

Johnson said the Working Group would like to discuss an extension of the time to develop the new Model #674 due to the sheer volume of comments received on Version 1.2 from July 11 through Aug. 8 and the number of requests for private calls with trade associations, consumer representatives, and companies.

Johnson said the 15 comment letters received prior to the July 28 due date are posted to the Working Group's web page and the meeting platform in the Summer National Meeting Event App. She also said the eight comment letters received after the July 28 due date will be posted to the Working Group's web page following the Summer National Meeting. She said the Working Group received 32 separate comments and redlined language documents in total. Additionally, she said the Working Group needs to review previously received comments to ensure all comments have been considered.

Johnson said extending the timeline would give the Working Group the time it needs to review all the comments submitted and have conversations with those who submitted the comments to ensure all stakeholders are heard and all parties understand the functional differences between different licensees and the various types of insurance being offered to consumers.

Johnson said the next version of the draft would be a redline that includes comments submitted, and the exposure draft period would allow a reasonable time of four to six weeks to review and comment on it. She said the Working Group will probably have another interim meeting before the Fall National Meeting, when a new timeline will be presented. Crow read a statement indicating that more work and time is needed for the state to support the draft model. Hastings thanked the Working Group for all its efforts in drafting a model that could work for all stakeholders, and she said Indiana has concerns that the interested state insurance regulators will work with the Working Group to resolve.

5. Discussed the Sections on Marketing, Consumer Notices, and Opt-Out/Opt-In in the Second Exposure Draft of Model #674

Johnson said the next item on the agenda is to discuss the topics on which the most comments were received; i.e., marketing, consumer notices, and opt-in/opt-out. She said the Working Group would hear from anyone who would like to talk about these topics. She asked that each stakeholder limit their comments to three minutes if possible and please focus on what, in their opinion, works and what does not. She said this will give Working Group members and other state insurance regulators time to ask questions and discuss the issues presented. Marnell reiterated the comments he submitted on the first exposure draft of the model prior to the Working Group's interim meeting in June, indicating that South Dakota could not support Version 1.2 of the model in its current form. Swanson said Nebraska agreed with the comments submitted by Marnell.

Shelby Schoensee (American Property Casualty Insurance Association—APCIA) said she appreciates all the hard work the Working Group put into Version 1.2 of the model, but she is disappointed that it did not include all of the APCIA's comments from the interim meeting in June. She said it was a patchwork of extensive regulatory changes that included unworkable notice requirements, such as obtaining consumers' signed consent for insurance data retention, sharing, and annually renewable data review, so it needs more work.

Kristin Abbott (American Council of Life Insurers—ACLI) said the drafting group was clearly dedicated given the tremendous amount of work that had already been accomplished, and she said she appreciated working with the drafting group on specific issues of concern to her members. She said, however, that a redline document would allow the most constructive feedback to be given to avoid conflicting verbiage. She also said she was extremely disappointed that the ACLI's ideas about JMAs, marketing, retention, deletion, and data correction had not been included.

Karrol Kitt (University of Texas at Austin) said state insurance regulators need to know that consumers need this revised model desperately, and consumers need their help in protecting personally identifiable information because most insurance consumers do not understand the implications of what happens to their data once companies share it with other non-insurance companies.

Lauren Pachman (National Association of Professional Insurance Agents—PIA) said she submitted comments on behalf of the PIA's members last week and was surprised that the adverse underwriting decision language had been kept in Version 1.2 of the model. At the interim meeting in June, she said she asked that the National Flood Insurance Program (NFIP) be fit into the draft model because only 10% of consumers buy flood insurance directly through the NFIP. Agents are selling it to the other 90% of consumers through an arrangement with the federal government—via federal government borrowing money or the Federal Emergency Management Agency (FEMA) through upstream and downstream agreements—that could be considered a JMA in this model. Pachman said most flood policies sold cover $250,000, and agents sell flood insurance for homes over that amount to ensure full coverage for homeowners. She asked how agents could offer this excess coverage under the model and if agents would need to get the consumer's approval in advance via written consent, which would be a potential errors and omissions (E&O) problem for consumers.

Johnson said she would be happy to set up a call with Pachman to discuss the sale of flood insurance further, as this concern was an unintentional consequence. She said she still believes state insurance regulation is better for consumers than federal regulation. Diederich said he believes the model has the same definition of financial institution as the federal government. Johnson confirmed that it is in Version 1.2.

Harry Ting (Health Consumer Advocate) said the new state insurance regulatory protections are sorely needed. He said the model is not confusing to consumers. For Sections 9 and 10 of Model #674, he suggested creating a standard template for consumer notices that could be clearly understood and uniform; i.e., like those created for the Medicare program.

Matthew J. Smith (Coalition Against Insurance Fraud—CAIF) said he submitted written comments on July 27 and urged state insurance regulators to update the model to protect consumers against insurance fraud. He asked the Working Group to focus on two issues: 1) consider making sure investigations of insurance fraud can continue by taking care not to prevent such investigations inadvertently; and 2) take the opportunity to designate fraud prevention clearly.

Peter Kochenburger (Southern University Law School) said he supports the revision of the model and understands that whether consumers should be given the opportunity to opt-in or opt-out of sharing their personal information is always the question. He said opt-in should be the default because opt-out means companies will share a consumer's personally identifiable information with their affiliates. Industry understands this, so that is what they prefer. Kochenburger said it is up to the Working Group to determine if consumers can have the protection of an opt-in consent that would provide the opportunity for consumers to know what they are agreeing to. He said he recently signed up for the highest level of Wi-Fi access, and the acceptance of the terms included several pages of legalism in very small print that was hard to read, even for an attorney. He said the only realistic opportunity for consumers to control the use of their data is an opt-in consent form. Kochenburger said the creation of an opt-in consent form is a complicated topic that needs further consideration. He said the Working Group has done a great job of putting together real consumer protection provided through state insurance regulation, whereas the federal government could adopt a broad bill.

Diederich said due to the GLBA, JMAs make it difficult to do this, and he needs ideas from Kochenburger on banks.

Wes Bissett (Independent Insurance Agents & Brokers of America—IIABA) said his members have threshold concerns, and he agrees that privacy is important, as is uniformity. He said the disagreement is on how to do it. He said the GLBA is wonderful, and the Working Group needs to use it. He said he has carried a lot of water for state insurance regulation over federal insurance oversight throughout the years because he supports state insurance regulation. However, he said he believes the Working Group should discontinue drafting a new model to replace the *NAIC Insurance Information and Privacy Protection Model Act* (#670) and the *Privacy of Consumer Financial and Health Information Regulation* (#672). He also said Model #670 and Model #672 only need minor adjustments, as they have worked well for many years.

Amann said she was actively involved when Model #672 was drafted in 1992, and the new model is being conscientiously drafted with language referred from Model #670 and Model #672. She said it would be helpful if Bissett could tell the Working Group where exactly it went off the rails because lines of business are different, as are companies' business processes. She also said new technologies have been and are being brought to the table, which is why the Working Group would appreciate any direction regarding Bissett's members' concerns.

Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) said she appreciates the drafting group's willingness to discuss issues of concern in the model with her members. She highlighted the importance of making the new model more workable for companies, and she asked that it be more like California's privacy regulations. She pointed out that the timeline in Section 5 of Version 1.2 is three times longer than it is in California; instead, it should be in alignment with California, like railroad tracks, rather than trying to change the entire landscape of privacy, which would take a major effort on the part of insurance companies. She asked if there was any need to go beyond what California or Model #672 did, particularly Sections A.6 and A.7 of the new model. She said these sections address marketing across jurisdictions, which should not be a topic for a privacy discussion. She said her members continue to be willing to work with the Working Group to revise the wording in Version 1.2 to address these outstanding issues.

Erica Eversman (Automotive Education & Policy Institute—AEPI) said she echoes the thoughts of the other consumer representatives, and she suggested specifically identifying certain types of data categories by looking to California, as companies are already complying with it. She said other personally identifiable information, such as commercial, financial, banking, internet, browsing, fingerprints, voice prints, geo data, audio, visual, education, and professional/employer information, should be considered as inferences that industry could use to create a profile that could lead to automotive insurance disputes. She said bodily injury under personal injury protection (PIP) auto insurance requires that the consumer waives federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) rights to give access to health information for claims. She asked if this gives other companies access to medical data that they would not normally have due to HIPAA protections.

Eric Ellsworth (Consumers' Checkbook) said he is a data scientist with both an information technology (IT) and a HIPAA background who believes in strong data protection. He said there has been a lot of discussion about the inability of companies to access data in legacy systems to correct or delete a specific consumer's data when it is no longer needed. He said while it is true that legacy systems require a lot of maintenance and a lot of work, it is not true that data in legacy systems is safe because companies cannot access it. He said an experienced data scientist can access data located anywhere and from any type of system, including a legacy system. He said it is also true that companies may not know what data they have or where the data they have accumulated, especially through agreements, mergers, and acquisitions of blocks of business from other companies, is located. He said contrary to what is being said about consumers having to pay higher premiums to cover the additional costs companies will incur to comply with the new privacy act, history has proven that not to be the case. He said the same thing was said about HIPAA and California's privacy law, yet neither HIPAA nor California privacy compliance has bankrupted any insurers. He said state insurance regulators need to bind companies to the same rules as HIPAA, and he encouraged state insurance regulators to maintain this level of control over consumers' data.

Diederich said the Parliament of India recently enacted very strong data privacy protections with a data fiduciary requiring consent. He said this is a level setting, as the U.S. is very technologically advanced but not very advanced in privacy protection.

6. Discussed Other Matters

Johnson reminded attendees about the Insurance Summit, Sept. 11–14.

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

SharePoint/NAIC Support Staff Hub/Committees/H Committee/2023 Summer/WG-Privacy/2023 Summer National Mtg/Minutes_Summer 23 NM_PPWG.docx

Draft: 8/8/23

Privacy Protections (H) Working Group
Conference Call
July 25, 2023

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met July 25, 2023. The following Working Group members participated: Katie Johnson, Chair (VA); Cynthia Amann, Vice Chair (MO); Damon Diederich and Jennifer Bender (CA); George Bradner and Anthony Francini (CT); Erica Weyhenmeyer (IL); LeAnn Crow (KS); Van Dorsey (MD); Robert Wake and Sandra Darby (ME); Jeff Hayden (MI); T.J. Patton (MN); Santana Edison (ND); Martin Swanson (NE); Richard Hendrickson and Gary Jones (PA); Patrick Smock (RI); Frank Marnell (SD): Mike Walker (WA); and Rachel Cissne Carabell and Timothy Cornelius (WI). Also participating were: Doug Ommen (IA); and Garth Shipman (VA).

1. Discussed Comments Received on the Draft of Model #674.

Johnson said that the revised work plan dated July 10, 2023, is posted on the Working Group's web page and indicates that the exposure draft of the new *Insurance Consumer Privacy Protection Model Law* (#674) was distributed July 11 for a comment period ending July 28. She said it also lists Sept. 12 as the date that bi-weekly Working Group open meetings will resume to discuss comments received. Johnson said the Working Group will hear comments on the new Model #674, starting with those from NAIC consumer representatives. Karrol Kitt (The University of Texas at Austin) said she is good with the revisions to Sections 17–20. Harry Ting (Health Consumer Advocate) said he would submit written comments by the end of the week that would include replacing the 10-year time for companies to comply with consent, use, and deletion of consumer data requirements with a more reasonable time frame that would include exceptions to be granted by the Commissioner. He said opt-in and opt-out needed expiration dates that are consistent in each section, as consumers tend to forget to whom they gave consent two years ago. Dr. Ting said he agreed with discussions during the interim meeting that included changing notice requirements to the 11 categories defined in the California Consumer Privacy Act (CCPA). He said that he opposed the adverse underwriting decisions section of the model that would require consumers to send a letter to request the reason for such denial because doing so would cause unnecessary delays and effort by consumers. He also said the option for a private right of action needs to include some individual remedy for significant breaches like that in the CCPA. Diederich asked if expiration dates should be included for consent only or other areas of the model.

Jeff Klein (McIntyre & Lemon, PLLC and the American Bankers Association—ABA) said changes to opt-in and opt-out have been narrowed to not include financial institutions; sensitive personal information (SPI) now includes emails; and the sharing of information now includes publicly available information. He said the ABA benefited from the private calls with the drafting group and that they would suggest adding the *Privacy of Consumer Financial and Health Information Regulation* (#672) sections verbatim to avoid state and federal conflicts. He agreed with Wes Bissett's (Independent Insurance Agents and Brokers Association—IIABA) comment letter that the new Model #674 should consider the 13 state privacy laws that have already been enacted.

Helen Dalziel (International Underwriting Association—IUA) said the IUA represents alien insurers with NAIC surplus lines written and asked that adverse underwriting decisions exclude lawful surplus lines because the definition of a licensee means that there is a relationship with companies, not with consumers but that brokers licensed to sell these should send notices to individual consumers. She said Article 3 (8) A (2) needs to include surplus and excess lines.

Jennifer McAdam (American Council of Life Insurers—ALCI) said the ACLI supports changes to private right of action and that the ACLI still has concerns with the new Joint Marketing Agreements section and the annual review of consumer data. She said the time to comply with the requirement to move away from legacy systems should be extended to 20 years and that the delivery of notice requirements needed to be modernized. McAdam expressed concern about the time left in the work plan and the amount of work still needed. She said ACLI members have been meeting weekly to discuss changes in the new model, and sometimes they meet more often. McAdam said more explanation is needed from drafters as to why the changes suggested by the ACLI were not made. She said ACLI members agree that progress has been made but that the language is unworkable for their members as revised.

Diederich said the Working Group wanted to make sure the legacy system issue does not limit real-time response and deletion. He asked the ACLI what time frame would work from its standpoint, as 10 years seemed generous to him. McAdam said that thousands of policyholders have been their customers for decades, so ACLI members need more than 10 years to change the systems in which the data for those policyholders' is recorded. Johnson said the Working Group recognized that there are difficulties but that some companies said 10 years was plenty of time. Even so, she said the Working Group gave commissioners discretion for individual company exclusions or extensions and that specific suggestions as to the desirable time frame are needed.

Swanson asked how much it would cost companies to make this change and how much of that companies would pass along to consumers. McAdam said she did not know how much it would cost or how much would be passed on. Peter Kochenburger (Southern University Law School—SULS) said legacy systems are not upgraded as frequently and are more vulnerable to hacking, so there is a greater need to end legacy systems to avoid giving hackers access. McAdam said she did not know about the technical part of it but that she is not so much concerned about it as companies are still subject to the *Insurance Data Security Model Law* (#668). Kitt said legacy systems cannot make modifications, so companies will have to change them so that the cost would be there to replace the legacy system with a new system or to keep the old one updated. Johnson said that at the NAIC International Forum, she heard that the cost of maintaining legacy systems is tremendous but that they still have lost costs compared to new systems.

Sabrina Miesowitz (Lloyd's Underwriting) said surplus lines are different as they go through brokers, not direct to consumers, and that Lloyd's Underwriting agrees with the IUA's comments on adverse underwriting decisions. Shelby Schoensee (American Property Casualty Insurance Association—APCIA) said the APCIA received significant additional changes to the notice content and delivery; joint marketing agreements; definitions; and the cover letter's intent versus the changes made. removal of the sharing of data with overseas affiliates and the private right of action sections of the initial draft of the model. She said the APCIA will submit additional comments in writing but that they need more time to do so.

Bissett suggested the deletion of personal information, notices, etc., and that the Working Group step back to reassess if a new model could be adopted at state legislatures. He said the Working Group should add to a successfully operating framework already in place. Bissett asked what problem the model is trying to solve. He said the National Conference of Insurance Legislators (NCOIL) does not like nor support state passage of the new model. Bissett said the Working Group should limit its changes just to existing marketing models. He also said that the IIABA will oppose the new model. Diederich said the old models were written pre-digital and that the Working Group is trying to address new digital processes because under the federal Gramm-Leach-Bliley Act (GLBA), there was no right of access, limited joint marketing agreements, and limited control of what happens to a consumer's personal information. Bissett said the U.S. House Committee drafted a new module to the GLBA with changes to consumer notices that indicated consumer data uses should be addressed. He also said that no new types of data have been used since then. Diederich asked Bissett if he had any guardrails to suggest so all parties could find a middle ground. Bissett said not having to disclose uses of client data and removal of the mandatory deletion within

90 days after the consumer is no longer a client takes away the agent's rights. Bissett suggested the Working Group see the New York State Department of Financial Services' (DFS') cybersecurity regulations.

Johnson said she disagrees with Bissett because the model has several reasons under which agents can keep consumer data. Bissett said the words on the page say consumer data can be kept while there is an ongoing business relationship, which he reads to mean that agents have 90 days after the policy closes. Johnson asked Bissett to give the Working Group language that is clearer for use in the new model. Bissett said he would not provide any. Marnell said the Working Group is performing an important task but that his state would not support this draft of the model. He said he does not support it as a model and that the Working Group has not listened closely enough to industry. Marnell said the model needs lots of redrafting, as noted in the redline he submitted. Swanson said he agreed with Marnell and supports the changes noted in Marnell's redline submission. Swanson said he thinks this is true in a lot of other states.

Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) said she appreciated the Working Group's attention to industry's comments. She said the Working Group has taken a novel approach with radical changes but that she likes the old system because Model #672 was a success of uniformity that just needs a few modifications to list third parties, allow deletions, and clarify permitted use of public information. Paolino said a pause is needed as she wants to understand why the Working Group has not made industry changes. Johnson said the Working Group still has changes needed and that the goal is to have a new redline draft (version 1.3) before the Summer National Meeting. She said the drafting group is still having private meetings because it still needs continual input to get to a workable model. Johnson said she disagrees that the new model is radically different and reiterated that the existing models needed changes, as noted by NAIC leadership and privacy working groups over the past four years. She said the goal is to develop a model that protects the privacy of consumers' data when it is used for insurance transactions. Johnson asked regulators, industry, and consumer representatives to submit ongoing specific wording changes to the model in redline because the Working Group reads all comments and takes parts of the language changes from everyone. She asked that interested parties read all the comments submitted and take note of the fact that they do not all agree on the wording, as each type of insurance and licensee has its own areas of concern due to differences in how their business is conducted. Johnson said the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) safe harbor is being revised as recommended by America's Health Insurance Plans (AHIP).

2. <u>Discussed Other Matters</u>

Johnson thanked everyone for their comments, discussion, and collaboration during the meeting. She said she looked forward to receiving additional comments on the draft and to continuing collaboration at the Summer National Meeting. She said the due date for changes on model 1.2 is July 28 and that comments received no later than Aug. 7 would be considered at that meeting. Johnson said the Privacy Protections (H) Working Group is scheduled to meet Aug. 13 from 11:30 a.m. to 1:00 p.m. PT (Pacific Time). She said there would also be a regulator-to-regulator meeting Aug. 12 from 4:00 p.m. to 5:00 p.m. PT. Both meetings will have virtual participation with the ability to speak (with requests submitted via the chat feature).

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

SharePoint/NAIC Support Staff Hub/H CMTE/2023 Summer/WG-Privacy/072523 Call/Minutes_PPWG Call_072523.docx

Draft: 8/9/23

Privacy Protections (H) Working Group
Interim Meeting
June 5–6, 2023

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met June 5, 2023, and June 6, 2023. The following Working Group members participated: Katie Johnson, Chair (VA); Cynthia Amann, Co-Vice Chair (MO); Chris Aufenthie, Co-Vice Chair (ND); Damon Diederich and Jennifer Bender (CA); George Bradner and Anthony Francini (CT); Erica Weyhenmeyer (IL); Justin McFarland (KS); Ron Kreiter (KY); Van Dorsey (MD); Robert Wake (ME); Jeff Hayden (MI); T.J. Patton (MN); Molly Plummer (MT); Santana Edison (ND); Martin Swanson (NE); Teresa Green (OK); Richard Hendrickson and Gary Jones (PA); Patrick Smock (RI); Amy Teshera (WA); and Rachel Cissne Carabell and Timothy Cornelius (WI). Also participating were: Doug Ommen (IA); Sandra Darby (ME); and Garth Shipman (VA).

MONDAY, JUNE 5, 2023

1. Discussed the Definition of Third-Party Service Providers Related to an Insurance Transaction, Third-Party Service Providers Not Related to an Insurance Transaction That Have Access to Consumers' Personal Information, and Contracts with Third-Party Service Providers

Johnson reminded attendees that these sessions are working sessions, and the Working Group would be focused on the drafting of model language. She asked everyone to be prepared to consider new language and offer their pros and cons. She said comments must be specific to the topic under discussion, and topics already discussed in open meetings would not be revisited during this meeting. Diederich said the Working Group has heard a lot about individual companies' excellent oversight of service providers and strong contractual protections with respect to these arrangements. He said the Working Group has asked for contract language but has not yet received it. He said the Working Group would appreciate the submission of language or standards for consideration and a set of best practices that the Working Group could apply to third parties.

Wake said state insurance regulators want to make sure promises that service providers make to consumers remain in place when data is shared. In addition, he said insurers should ensure that their promises made to consumers are upheld by the service providers who are provided access to the data, as the type of data shared may require different protections. Swanson said Nebraska could not offer up this model as is as a bill in the legislature. Aufenthie asked about third parties who get consumers' personal information from the insurer and who do not have a contract with the insurer in the classic tow truck example. He asked to what extent state insurance regulators can require an advance contract for every type of situation, or whether it should be stated that the state department of insurance (DOI) has jurisdiction. Then, if the tow trucks go beyond what they need to do for the claim, it is criminal theft. Wake said this is where privacy meets security. Chris Petersen (Arbor Strategies LLC and the Coalition of Health Insurers) asked if the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) safe harbor applies. If it does, he said the Business Associate (BA) rules would apply. Without knowing whether that applies, he said the Coalition of Health Insurers would push for privacy regulation that looks like the HIPAA Privacy Rule so that health plans that already comply with HIPAA would follow these rules and everyone else would have different rules. He said there is a distinction between a breach and misuse of information, so this is a security versus privacy issue. He said in the HIPAA world, the BA is responsible for any misuse, and under the safe harbor, the state DOI could determine if there are enough of those violations so the entity is not complying with HIPAA. Then, the safe harbor would disappear, and the state DOI could go after them.

Katie Koelling (Thrivent Financial) said there is a difference between privacy and security, so imposing the same obligations on all types of vendors is not possible. She said Thrivent Financial is legally required to perform third-party due diligence, and it uses a third-party due diligence questionnaire. She said she believes the model should be more risk-based than prescriptive. Peter Albert (Progressive) said: 1) care needs to be taken toward accurately defining what a service provider is; 2) there need to be exceptions; and 3) redundancy within existing laws needs to be avoided. He also said when Progressive dispatches a tow truck, it does it through third parties with whom it already has contracts. Wes Bissett (Independent Insurance Agents & Brokers of America—IIABA) said the model has significant problems because the definition of a third party includes licensee, and it should not because it treats agent/insurer relations as a third-party relationship, which is not the case. Therefore, the definition should not include licensee. Bissett also suggested referring to the definitions in the National Institute of Standards and Technology (NIST) as an amendment to the federal Gramm-Leach-Bliley Act (GLBA). Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) said the contract management process is a big lift and takes a lot of work, so the Working Group should consider grandfathering for contractual provisions and include wording in an appendix about third-party contracts, safe harbors, and compliance. Lauren Pachman (National Association of Professional Insurance Agents—PIA) said the internet requires that consumers accept terms and conditions, and consumers opt into the internet. Kristin Abbott (American Council of Life Insurers—ACLI) said the ACLI will submit specific language. Jessica Waltman (National Association of Benefits and Insurance Professionals—NABIP) said a safe harbor for HIPAA should extend to the whole model or as a standard for all insurers because it is a known entity, so it would be easier for vendors to follow where there is a power imbalance. Al Sand (Committee of Annuity Insurance) said the contractual language around third parties makes it so licensees do not choose the best third party but rather the ones who will agree to the contract language.

Johnson asked if there were some groups of third parties that should be treated differently than others. Petersen replied that those with incidental exposure should be. He said there should also be differences between first-party data and second-party data when the first relates to getting insurance and the second relates to non-insurance, such as tow truck vendors. Koelling said the definition is too broad because it does not include a person who obtains a consumer's information, and she said she would send a suggested definition with exclusions to address it.

2. <u>Discussed Definitions of Insurance Transactions and Additional Permitted Transactions</u>

Tricia Wood (Liberty Mutual) said that normal processing activity should be reasonably anticipated by a consumer, and the model should include language that covers business purpose catchall. She said there should not be an opt-out for any part of an insurance transaction; however, she said for additional permitted transactions (APTs), there needs to be an opt-out provision. Shelby Schoensee (American Property Casualty Insurance Association—APCIA) said the definition of information technology (IT) is too narrow. She said in Article §2, Section 4(B), the uses of data should be included, and any mathematical-based decisions should be deleted. Aufenthie said this was included to cover artificial intelligence (AI) and APTs, but it does not think the existing language captures the intent. Petersen said he does not believe "by or on behalf of licensee" works because disclosures are permitted that do not fall under that; i.e., sharing with law enforcement. Albert said the IT definition is too narrow, and he suggested that the Working Group reflect on existing model definitions because certain marketing actions may fall under IT. He said if an insurer is giving data to their own affiliates to offer supplemental coverage, the transaction should not be subject to opt-in or opt-out. He said APTs and product development should be included in this category as well. Bissett said IT, as used in Section 4A(1), says personal information (PI) cannot be collected, processed, or shared unless it fits into categories in the definition of IT. He said the federal Fair Credit Reporting Act (FCRA) preempts some of this, including the exchange between affiliates, and it is an unconstitutional restriction of free speech if IT is content or speaker-based. Jennifer McAdam (ACLI) said if IT means any transaction or service by, or on behalf of, licensees, the Working Group should add "or affiliates" and "or any functions that support the above." She also said marketing is important for consumers to be supported in a holistic manner. Paolino said opt-out is the only approach that makes sense for APTs, such as research activities and product development, so it makes sense to include, and there could be more areas to expand upon, such as internal analytics. Sand said updating data is difficult and puts insurers at a competitive disadvantage. He said a better framework would be to focus on consumer empowerment and not try to figure out ahead of time what is appropriate to offer to consumers. McAdam asked what revelations the Working Group has been having or bad practices the Working Group has seen. Johnson said there is always someone who wants to push the envelope, and state insurance regulators need the power to rein them in when that happens. Harry Ting (Health Consumer Advocate) said regarding the company's comments about future developments and products, the consumer cannot know what to consent to when the consumer does not know what these future products could be.

3. Discussed Marketing Insurance Products to Consumers Using Consumers' PI, Marketing Other Products to Consumers Using Consumers' PI, and Affiliate Marketing

Johnson said the Working Group is concerned about companies marketing something other than insurance and inundation of unwanted ads on consumers. Petersen said there is a need for a definition of marketing. Sand said restrictive marketing standards will put insurers at a competitive disadvantage. He said consumers may not be opposed to marketing, but they may not take the time to give consent if there is an opt-in standard. He said this will lead to a competitive disadvantage, and it is especially problematic for annuity companies when a broker/dealer is also marketing a competitive product, such as a mutual fund. He said consumers need to be made aware of all products, and it is not fundamentally bad to make consumers aware of insurance products. Wake said the issue is how to get to reasonable limits so consumers are not inundated with marketing materials. He said the opt-out notice might be a good marketing opportunity, where a company could tell a consumer what information they might be giving up by opting out.

Sand said limiting information to consumers does not create a more informed consumer. He said it is better for a consumer to be contacted and then allow the consumer to tell the insurance company they do not want to receive additional marketing information on a particular topic or product. He also expressed concerns with Section 4G. Albert said restrictions on marketing are unworkable. He also expressed concerns with the ambiguity of the term "marketing." He said the focus should be on insurance-specific marketing concerns, insurers should be able to market products without consumer consent, and there should be an opt-out standard consistent with existing federal law. He provided an example of how an insurer could not obtain affirmative consent to market an insurance product to a consumer who does a Google search for "I want cheap car auto insurance." He said an opt-in standard would also prevent an insurance company from mailing a consumer an offer for home insurance after a consumer's purchase of a home. He said if an insurance company is sharing information with an affiliate, the company must offer the consumer an opt-out under the FCRA. He said Progressive has affiliates throughout the U.S., but the affiliates share one database. Pachman expressed concerns about restrictions on marketing and gave an example of flood insurance coverage and the potential inability of an agent to market home insurance coverage to provide greater than the $250,000 coverage offered through the National Flood Insurance Program (NFIP).

Johnson asked what, if anything, agents should be prohibited from doing. Pachman said selling a consumer's data without their consent should be prohibited. Johnson asked if an agent should be prohibited from having the ability to sell products other than insurance to a consumer. Johnson replied that it is important to identify what product is related to an insurance product. She said one way to make this determination is to determine if the related product is tied to risk mitigation. She said state insurance regulators are okay with the sale of additional products, but they do not want an insurance agent to sell information to a company selling canoes, such as Land's End, after the purchase of a lake house.

McAdam said prior consent language will deny consumers the opportunity to learn about products and services. Glenn Daly (John Hancock) said this is a data-driven world, and he suggested the development of a one-pager for consumer education. Paolino said that risks evolve for consumers, and technology is continuing to change, so state insurance regulators should think about this as the model framework is developed. Bissett said the definition of marketing is important, but the more important question is whether we are looking at an opt-in standard for marketing. Wake asked if do-not-call lists are unconstitutional. Bissett said he believes there would be a problem if a state adopts a law saying only insurers cannot market, but everyone else can, and this would be considered a discriminatory standard.

4. Discussed JMAs with Affiliates and with Non-Affiliated Third Parties

Abbott said a prohibition of joint marketing agreements (JMAs) by affiliates would be problematic, and standards for joint marketing should be the same for all financial institutions. Schoensee suggested keeping the joint marketing structure in the *Privacy of Consumer Financial and Health Information Regulation* (#672). Sand said he read the six elements of joint marketing from Model #672, and this reflects the fact that smaller institutions will not be able to offer all products. He said joint marketing allows the offering of a larger option of products, and joint marketing allows insurance products to be brought to consumers that would not otherwise be offered. Wake asked why an opt-out standard for joint marketing is not appropriate. Sabrina Guenther Frigo (CUNA Mutual Group—CUNA) said CUNA partners with credit unions to bring products to consumers, and joint marketing standards should be the same across all financial institutions. Johnson asked if banks give CUNA a list of names for marketing and if then the consumer can opt out after the initial offer. Guenther Frigo said this is the case. Aufenthie asked whether CUNA gets information from a credit union and if then a consumer can opt out of marketing. He also asked if CUNA then honors the request and deletes the consumer's information. Guenther Frigo said CUNA honors the consumer's request, and the deletion of consumer information is based on legal requirements.

TUESDAY, JUNE 6, 2023

5. Discussed Opt-In vs. Opt-Out Consent to Marketing and the Difference Between Marketing Insurance and Non-Insurance Products

Schoensee expressed concerns about moving to opt-out. She said opting out makes it difficult to identify coverage gaps and for insurers to conduct business. Wake said marketing is generally an opt-out standard, but there is an opt-in for health under both the GLBA and Model #672. He asked what people think about opting out of marketing and opting in for the use of sensitive data that is appropriately defined. Wood said cookies are attached if a consumer accesses the company's website. She said the cookies notify the company if the consumer goes to another website so the company can place an ad on the other website. At the same time, though, she said the company does not have any information about the consumer. She also said California has an opt-out regime for cross-context and behavioral advertising, and she encouraged consistency with the California standard.

Diederich asked if anonymized data ever becomes associated with an individual. Wood replied that it does not, and any information associated with an individual would come from the customer and not from the cookie. She said the company only knows that a consumer came to their website. Albert said Facebook and other tech companies have a lot of information about consumers. He said Progressive will attach cookies to take a consumer back to its web page, but Progressive does not know anything else about the consumer. He said there are also third-party cookies being dropped by Amazon, Google, and Facebook. He said if Progressive is interested in a certain consumer profile, Progressive puts the information through a hashing program. He said service providers, like Google, know other websites that a consumer has visited, and Progressive can then work with the service providers to obtain a list of consumers who might be interested in insurance products. He said service providers track consumers across all websites. He also said insurance companies need a consistent standard across all states to eliminate redundancies and consumer confusion. Aufenthie asked why Progressive did not apply standards of the California Consumer Privacy Act (CCPA) to all states. Albert said the CCPA is a complicated law, and Progressive is still working through its implementation of it to assess the impact on its business in California. For example, he said when a consumer requests the deletion of information, it leads to the manual deletion of the information at Progressive, which is a complicated endeavor. Wake suggested using opt-out for marketing except for certain types of data. He said this is a regulatory regime worth exploring; i.e., carve out certain types of sensitive information, such as health information, from the opt-out standard. Albert suggested caution around carving out health information because a property/casualty (P/C) company settling a claim would need access to health information. Wake suggested an opt-out regime for general marketing purposes but to carve out specific sensitive personal information to be under an opt-in regime. He also suggested defining sensitive PI as it is in the *NAIC Insurance Information and Privacy Protection Model Act* (#670) when companies use precise geo-locations to adjust a consumer's insurance rate when hard accelerations, late-night driving, etc., result in higher risk factors or for ancillary services like dispatching emergency services.

Paolino said an opt-in approach for marketing would make insurance an exception and put less information in the hands of consumers. Sands said it is important to maintain a level playing field within the financial services industry. He said an opt-in approach for marketing would limit the marketing of annuities compared to mutual funds. Johnson said the Working Group heard industry wants a level playing field, and opt-ins are difficult. She asked if any insurance companies use sensitive information for marketing. Daly said he is concerned about the broad definition of sensitive information in the current draft. He said opting in and the need for consumer consent would inhibit companies from providing products to consumers, especially personalized products.

Diederich asked what type of sensitive information is being used in marketing for diversity, equity, and inclusion (DE&I). Daly said an example is LGBTQ data. Diederich expressed concerns about what information a consumer wants to be available to the public and what information they want to keep private. Daly agreed but said there is a need to maintain a level playing field so insurance products that consumers need can be made available to those consumers. Wake agreed but said there is a need to balance benefits and harms. Daly said companies respect what they know about consumers and reiterated companies' need for a level playing field. Teshera asked what marketing information is provided. Daly said every consumer's mobile device is segmented in the advertising world. Daly said a company can then identify what segment of the market they want to target with their advertising because advertising and marketing is a very complicated process that begins when a consumer query is captured in the data world. He said this does not mean the consumer is identified, but it does mean a company can identify a consumer's interest for marketing purposes. Daly also said the definition of sensitive information is very broad in the current draft of the model. Diederich said cross-contextual advertising is anonymized, and he asked if companies need individual consumer information. Daly responded that they do not need individual consumer information.

6. <u>Discussed the Contents Necessary to Have in a Notice of Consumer Privacy Practices</u>

Albert said privacy notices are complicated because the content is mandated by state insurance regulators, and he suggested selecting one of the abbreviated disclosure notices from Model #672 to avoid the requirements of privacy notices that contain more prescriptive statements. He said privacy notice requirements should specify what categories to cover but should not become too prescriptive. For example, he said Progressive discloses that information is shared with rental car companies rather than listing the names of each specific rental car company. He is concerned with the use of wording like "specific types" because it sounds like state insurance regulators want an exhaustive list.

Schoensee suggested that the Working Group add a safe harbor for companies using federal privacy forms. Sands said if disclosures become too specific, it will be difficult for companies to comply, and generalized disclosures that are principle-based would be more appropriate. He said the current language of Model #674 would prohibit insurers from using the federal privacy form, and he questioned what consumer benefit is derived from the disclosure of a specific service provider's name rather than disclosure of a broader category of service provider that provides "x" services. Diederich said the names of specific providers help consumers track where information goes in case there is a service provider breach. Sands said there are other state laws regarding notification of breaches. Wood said a privacy risk is not best addressed through privacy notices to consumers, especially with a detailed list of specific vendors, because the notices would become inaccurate very quickly if specific vendors are required to be listed. She said the posting and disclosure of vendors also increase the security risk for a company, and a vendor may also consider its contract with a company to be confidential. Diederich asked if companies would make the names of specific vendors available to consumers upon request. Wood said they would not because while this request sounds reasonable, such disclosure may not be a good idea. For example, she said a company may use Amazon Web Services (AWS), and AWS does not do anything with the data. She asked why the company would need to disclose it. Similarly, she asked why it would be necessary to disclose the name of a vendor used for a company's accounting. She also questioned how this would benefit a consumer because the company would not change the use of certain vendors due to its business needs.

Paolino encouraged the use of a safe harbor for sample notices and continued the use of the federal privacy forms that are included by reference in Model #672. Petersen questioned the usefulness of a notice unless a consumer can do something in response to the notice. He said this is not the case today with privacy notices given to consumers, as the notices simply disclose that the company uses personal information in compliance with current law. Johnson said a consumer can switch companies if they do not like how a company is using their data. Petersen said price point, company reputation, and service usually drive consumer behavior, and he questioned whether a consumer would change companies based on information in a company's privacy notice. Wake said even if a consumer may not be able to do anything, a consumer may still want to know, and that it is also important for them to know if a company has a policy more restrictive than what is permitted by law. Daly said disclosure of specific vendors will increase the privacy risk to customers.

7. Discussed the Frequency and Methodology of Delivery for the Notice of Consumer Privacy Protections

Schoensee said the timing of notices should be consistent with the direction provided in the NAIC's most recent privacy bulletin from 2016 that incorporated the federal Fixing America's Surface Transportation (FAST) Act amendments regarding the frequency of privacy notices. She also has concerns with notices that might be required for group insurance, reinsurance, and the need to include beneficiaries in notices because this could lead to the premature disclosure of a consumer's estate plan. Johnson asked if the model should allow consumers to continue receiving notices via paper delivery. Paolino encouraged guidance on the timing of notices set forth in the FAST Act. She also suggested consideration of how a group of companies may interact and send notices on a consolidated basis. Diederich asked about potential conflicts with the Uniform Electronic Transactions Act (UETA) and its requirement for companies to receive consumers' affirmative consent for electronic transactions. Dorsey said electronic notice would also violate Maryland law. Johnson said the Working Group may look at a requirement of paper notice for the initial notice and then for companies to provide consumers with an option to opt out of paper notices in the future. Daly said consumers without internet access can call the company, and any company using beneficiary information for marketing should have disclosed this in their initial privacy notice.

8. Discussed Other Matters

Jeff Klein (McIntyre & Lemon PLLC) asked procedural questions on the next draft because the GLBA was about much more than privacy. He said no state may prevent or significantly interfere in insurance sales or cross-marketing, and there are 13 safe harbors outlined in the GLBA. He also said the current draft of Model #674 raises preemption issues. Johnson asked companies to let the Working Group get the next draft out, as it may address many of these issues. McAdam asked if the notice provisions would apply to reinsurers or group insurance, as the current provisions require them to provide consumer notices. Johnson said the Working Group is not going to require reinsurers or group insurance to provide consumer notices in the next draft. Dr. Ting asked the Working Group to include special safeguards in notices to maintain privacy in cases of domestic abuse.

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

SharePoint/NAIC Support Staff Hub/H CMTE/2023 Summer/WG-Privacy/Interim In Person PPWG/Minutes_PPWG Interim Mtg_060523-060623.docx

© 2023 National Association of Insurance Commissioners

Draft: 5/22/23

Privacy Protections (H) Working Group
Virtual Meeting
May 16, 2023

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met May 16, 2023. The following Working Group members participated: Katie Johnson, Chair (VA); Cynthia Amann, Co-Vice Chair (MO); Chris Aufenthie, Co-Vice Chair (ND); Chelsy Maller (AK); Gio Espinosa and Catherine O'Neil (AZ); Damon Diederich (CA); George Bradner and Hicham Bourjaili (CT); Ron Kreiter (KY); Van Dorsey (MD); Jeff Hayden, Renee Campbell, Danielle Torres, and Julie Merriman (MI); T.J. Patton (MN); Molly Plummer (MT); Santana Edison (ND); Connie Van Slyke (NE); Teresa Green (OK); Scott D. Martin (OR); Gary Jones and Richard Hendrickson (PA); Matt Gendron and Raymond Santilli (RI); Frank Marnell (SD); Shari Maier and Michael Walker (WA); and Timothy Cornelius, Rachel Cissne Carabell, and Barbara Belling (WI). Also participating were Janice Davis, Scott Woods, and Rebecca Smid (FL); Paula Shamburger (GA); Joseph Fraioli and Sonya Sellmeyer (IA); Hermoliva Abejar (ID); Tanji J. Northup (UT); Garth Shipman (VA); and Mary Block and Karla Nuissl (VT).

1. <u>Discussed Sharing Consumer Information with a Person Outside the Jurisdiction of the U.S., Section 4. A (5)</u>

Johnson said the Working Group would discuss the sharing of consumer information with a person outside the jurisdiction of the U.S., including the consent provision (Section 4. A (5)) and the guardrails around sending consumer information outside the jurisdiction of the U.S.

Chris Petersen (Arbor Strategies) said he has legal and political concerns about this provision. He said that he believes federal labor laws pre-empt this type of provision at the state level and that this is a security breach issue rather than a privacy issue. Petersen said companies are becoming global and recommends that this provision be stricken from the model. Sarah Wood (Insured Retirement Institute—IRI) reiterated the comments in the IRI's letter. She said this provision would disrupt annuity supply chains by being overly burdensome in requiring operational changes, so implementation would not be feasible. Johnson asked Wood if she was referring to costs being prohibitive. Jordan Heiber (U.S. Chamber of Commerce) said its members are concerned with this provision as drafted because it would limit or prevent companies from outsourcing functions, prevent access to information, and lead to increased costs that would be passed on to consumers. He said mandatory consent requirements would confuse companies and consumers as to what information is needed. Heiber said it conflicts with U.S. legal, contractual, and recent state legislation in California and other states. He said these requirements are unnecessarily restrictive and conflict with the G7 requirements in the Organisation for Economic Co-operation and Development (OECD), which is moving forward with its plan for the free flow of data and trust globally.

Kristin Abbott (American Council of Life Insurers—ACLI) said this provision appears to give consumers consent. However, in her April 3 comment letter, she said it is better for companies to address consumer consent questions through vendor oversight and contractual obligations. She said this provision would severely limit global insurers and reinsurers, as well as cause them to lose 24/7 customer service. Abbott also said that the *Insurance Data Security Model Law* (#668) already covers this, so she suggests the provision be removed from the new model, *the Insurance Consumer Privacy Protection Model Law* (#674). Sabrina Miesowitz (Lloyd's of London—Lloyd's) said the comment letter Lloyd's submitted included a definition of "licensee" that includes unauthorized insurers like Lloyd's, which are non-U.S. based. She said this is different from other models in that most models say this means "surplus lines licensees." Shelby Shoensee (American Property Casualty Insurance Association—APCIA) said this provision would ban global servicing, as it goes against the G7 financial dialogue. She said the protection of data is a function of both security and systems and is concerned it would block a company's functionality, even within the company itself. Shoensee said it would cause companies to become less efficient over time and would limit a

© 2023 National Association of Insurance Commissioners

company's ability to respond to subpoenas from outside the U.S.; therefore, the provision should be stricken from the model. Bob Ridgeway (America's Health Insurance Plans—AHIP) and Tom Smith (American Reinsurance Association—ARA) both said they agreed with the others who had spoken. Ridgeway said companies help consumers save money and that the risk is on the carrier if anything happens.

Joseph Whitlock (Global Data Alliance—GDA) said he represents a coalition of 70 companies that rely on data transfer around the world. He said there are three cybersecurity, fraud, and privacy concerns: 1) domestic; 2) international obligations; and 3) international policy. Whitlock said this provision is more restrictive than federal laws and that it raises Article 1 constitutional concerns, as well as international case law concerns. He said there are cross-data requirements, as the provision is more restrictive than in other countries or jurisdictions that have very strict laws with contract-based consent, like China, Vietnam, and Africa. Petersen said privacy is about how and when data can be used and what companies need to do to protect it. If a third party misuses data, it is a legal breach and, therefore, a security issue. He said there are two victims—the company and the consumer—and that the provision as written says, "as permitted in the U.S." (not outside the U.S.). Ridgeway said that the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) does not cover lots of information and that HIPAA data is controlled by contracts that are standard business association forms. He said companies could consent to jurisdiction, perhaps.

Diederich said he appreciated the comments and is sensitive to the concerns presented by companies and trade associations but that he was more concerned with consumer understanding and consent. With strong vetting, security, and contracts, he would like free-flowing data with trust. Diederich asked what the minimum boundary conditions, standards, and requirements would be to get companies to build out this type of system. Johnson said the Working Group has asked companies and trades for these types of industry standards many times. Diederich said state insurance regulators keep hearing that the carrier is the victim when data breaches occur and that the real problem is how to ensure there are safeguards on the front end. He said this is very helpful to build in protections for consumers in place of consent to prevent injury down the line. Silvia Yee (Disability Rights Education & Defense Fund—DREDF) said she would love to see a legal opinion that HIPAA has the authority over U.S. companies that operate overseas. She asked how companies can be held accountable because HIPAA is fairly limited as to what type of data is included.

2. Discussed Other Matters

Johnson reminded attendees about the in-person interim Working Group meeting to be held in Kansas City, MO, on June 5–6. She said the purpose of this meeting is to collaborate with state insurance regulators, consumer representatives, and industry members on revised wording for the most complex topics in the new draft of Model #674. Johnson thanked state insurance regulators, consumer representatives, and industry members who had submitted requests to be added to the registration invitation for this meeting, as the venue limits seating. Ridgeway asked when the agenda for the interim meeting will be available. Johnson said the agenda should be distributed and posted by May 22. Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) asked when the revised draft of Model #674 would be available. Johnson said a revised draft would be posted after the interim meeting and after the Working Group meets in regulator-to-regulator session. Schoensee asked about the logistics for the interim meeting. Johnson said the room would be set up like it was for the Working Group at the Spring National Meeting and that the attendees may break into table rounds to discuss issues separately should the need arise during the meeting. She said the Working Group will have suggested language to start the conversations and that Lois E. Alexander (NAIC) will distribute and post the dial-in information a week prior to the meeting for those who will participate in listen-only mode.

© 2023 National Association of Insurance Commissioners

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

SharePoint/NAIC Support Staff Hub/Committees/H Cmte/051623 Call/WG-Privacy/Minutes_PPWG_051623.docx

Draft: 5/23/23

Privacy Protections (H) Working Group
Virtual Meeting
May 2, 2023

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met May 2, 2023. The following Working Group members participated: Katie Johnson, Chair (VA); Cynthia Amann, Co-Vice Chair, and Jo LeDuc (MO); Chris Aufenthie, Co-Vice Chair (ND); Chelsy Maller (AK); Gio Espinosa and Catherine O'Neil (AZ); Damon Diederich (CA); Kristin Fabian, Hicham Bourjaili, Anthony Francini, and Kurt Swan (CT); Erica Weyhenmeyer (IL); LeAnn Crow and Shannon Lloyd (KS); Alexander Borkowski (MD); Jeff Hayden, Chad Arnold, Renee Campbell, Danielle Torres, and Julie Merriman (MI); Molly Plummer (MT); Santana Edison and Colton Schulz (ND); Martin Swanson (NE); Teresa Green (OK); Raven Collins and Thomas Hojem (OR); Gary Jones (PA); Patrick Smock and Matt Gendron (RI); Frank Marnell (SD); Shari Maier, Amy Teshera, and Michael Walker (WA); and Lauren Van Buren, Timothy Cornelius, Rachel Cissne Carabell, and Barbara Belling (WI). Also participating were Rachael Lozano and Rebecca Smid (FL); Joseph Fraioli (IA); Hermoliva Abejar (ID); Shelley Wiseman (UT); Rebecca Nichols and Garth Shipman (VA); and Mary Block, Karla Nuissl, and Isabelle Turpin Keiser (VT).

1. Discussed Confidentiality (Section 21)

Johnson said the Working Group would like to discuss the use of the *Insurance Data Security Model Law* (#668) confidentiality wording in Section 21 of the new *Insurance Consumer Privacy Protection Model Law* (#674).

Bob Ridgeway (America's Health Insurance Plans—AHIP) said he disagreed with the frequently asked questions (FAQ) because question one noted a slight difference, but the wording in Model #668 deleted one-third of the Own Risk and Solvency Assessment (ORSA) wording. He said AHIP had argued that "shall" should not have been changed to "may" in Model #668 when referencing regulators receiving written agreement (i.e., third-party), but instead to give notice only if subpoenaed on ownership. However, AHIP had lost that battle, so it was proposing limited language again, as Model #668 was less deserving of protection. Ridgeway said AHIP members want the longer language and reiterated the same arguments they had used during discussions of Model #668. Kristin Abbott (American Council of Life Insurers—ACLI) said the confidentiality of intellectual property must be protected to avoid infringement. For Section 21 C. 3 and Section 21 C. 4, she said the ACLI prefers the stronger ORSA provisions. Cate Paolino (National Association of Mutual Insurance Companies—NAMIC) said NAMIC would submit comments similar to those mentioned by the ACLI on using the wording from Model #668 in Model #674.

Birny Birnbaum (Center for Economic Justice—CEJ) said Section 21 should be deleted because consumers need to have access to any market conduct exam that is already considered confidential. The wording he suggested is that the privacy disclosure to consumers would be confidential if submitted to regulators and that the FAQ are proprietary because they apply to consumers, who need to be able to see what is being disputed by the company. Birnbaum said consumers need to be empowered to compare companies using all information, so nothing should be considered confidential or be kept from consumers' review.

Johnson asked those commenting to submit suggested wordings in writing following the meeting. She said the Virginia Bureau of Insurance is not subject to the federal Freedom of Information Act (FOIA), but Virginia laws are. Johnson said privacy policies must be posted on company websites. Teshera said records are not held in confidence in Washington state and that the department of insurance's (DOI's) responses are not held in confidence either. Diederich said the Working Group's intention was not that information automatically would be confidential simply because it was given to regulators.

2. Discussed Retention and Deletion of Consumers' Information (Section 5) and Record Retention (Section 22)

Johnson said the Working Group would discuss the retention and deletion of consumers' information wording in Section 5 and the record retention wording in Section 22 of Model #674 next. She said the Working Group intends that companies would be allowed to keep consumers' information for as long as it is needed, but they would delete it within 90 days of the date when it is determined the information is no longer needed to conduct the business with the consumer. She said private calls with companies before this meeting have indicated that this requirement is easy for new companies to do. However, it is very difficult, if not impossible, for companies with old, legacy-based systems.

Shelby Schoensee (American Property Casualty Insurance Association—APCIA) said the section regarding "applicable to any within Section 5 (A)" should be deleted, as well as changes to Section 5 (A) (1) and Section 5 (A)(9). She asked for redress from the 90-day requirement, as it is impossible for legacy companies especially. She also said that exceptions from the federal Gramm-Leach-Bliley Act (GLBA) 502 (b) are also needed and that she had similar concerns about Section 21 and Section 22. Jennifer McAdam (ACLI) asked how Section 5 (A) and Section 5 (B) (i) could be administered without being retroactive, especially with regard to in-force business with regard to information obtained prior to the effective date of Model #674. She noted that the ACLI would like to revisit this section later as others had indicated earlier. She asked that the Working Group add experience studies regarding company insolvencies to Section 5 (b) along with 90-day deletion concerns and the notice from the company on third parties, as the deadline is unfeasible and could damage financial reporting. McAdam suggested a risk-based approach with a reasonable amount of time, along with possibly considering wording similar to that in the California Privacy Rights Act (CPRA). She said Section 5 (b) (3) should read the same as the APCIA had indicated and that the ACLI would be submitting its additional comments in writing. Paolino said she agreed with what the other trade associations had provided.

Wes Bissett (Independent Insurance Agents & Brokers of America—IIABA) said the IIABA had several concerns with these sections, as the duty to remove data is very comprehensive with new concepts above what the federal requirement indicates. He wondered why the insurance industry was so strict compared to other non-insurance businesses. Bissett said he is worried that most states would not pick up nor pass such a model, so there would be no uniformity. He said Model #674 is a wholesale rewrite when a tune-up was needed—not a complete overhaul. Bissett said he agreed with the ACLI on Section 5 (b) (3), especially the requirement that small businesses need to control third parties that they do business with.

Diederich said the Working Group's job is to draft the new model so state insurance regulators can use it to regulate for the future. The old models were written several decades ago when legacy systems were written so data could not be deleted in order to avoid theft. He said that now it is known that any data can be stolen, and the only data that is theft-proof is data that is not stored. Deleted data cannot be stolen. He asked companies what state insurance regulators can do to help move them forward with new systems that replace the antiquated legacy systems. Johnson said the Working Group is looking for what would be workable, such as, perhaps, changing the 90-day rule to guardrails for licensees to use or de-identifying the data and keeping it.

Lauren Pachman (National Association of Professional Insurance Agents—PIA) asked how companies would determine when a consumer's data was no longer needed. Johnson said it would be up to the licensee to determine how long the data is needed. She said it would also be up to the licensee to write up their policy and follow it. Tricia Wood (Liberty Mutual Insurance) said, with regard to privacy and records retention, that there is a business purpose for the business records that they keep and that they are looking at not all consumer information. She also said they need a longer period to replace their existing systems.

Elizabeth Magana (Privacy4Cars) said she proposed keeping the requirements closer to the Internet of Things' (IOT's) data retention policy, which allows companies to keep the data as long as they have a legitimate business purpose. Jim Hurst said legacy systems were designed to be write once, read many (WORM), and kept forever, so historical data in such systems simply cannot comply with newer, more modern data privacy requirements. Patrick Simpson (Erie Insurance) said his company has a mix of legacy and new systems and that under New York cyber regulation, what may be feasible today should be periodically reviewed with plans for the future being brought to state insurance regulators, regardless of whether it is for a new system or changes to legacy systems. He said carriers do not want to keep legacy systems because it would not be competitive and because the more data a carrier has, the greater the risk to the company. Simpson said true de-identification would not permit re-identification. He said that as a property/casualty (P/C) insurer, Erie Insurance does have some legacy and some modern systems, as well as some changes from mainframe to cloud issues. He also said how long a change would take depends on the business, but on average, it could take less than 10 years. Hurst said he had no idea how long it would take to switch systems but that he would work to draft a final plan by the end of this year as a possibility.

Silvia Yee (Disability Rights Education & Defense Fund—DREDF) said she understood the need to maintain consumer data for claims. However, she said it seems the data to be collected is mammoth and that the carrier that gets the data can keep it forever. She advocated for a standard across the board so that consumers do not have to track down their data for every company or individual who gets it. Erica Eversman (Automotive Education & Policy Institute—AEPI) said companies need more modern equipment and systems that promote or incentivize the implementation of new technologies. Birnbaum said there is a need to have guidelines for implementing such technologies. Karrol Kitt (The University of Texas at Austin) said this is a technical issue and agrees with Simpson that legacy systems need to be replaced. Birnbaum said the infeasibility of taking data from a legacy system makes it even more imperative to strengthen the Model on the uses of consumer data due to the wide distribution of such systems.

Diederich said the new Model #674 must deal with the information being shared today, as well as with the new data that will be shared in the future. Johnson said some models have a step-up schedule with certain goals for the future and wondered if this type of schedule might work for the privacy model as well. Aufenthie said the question for those using a legacy or WORM system to answer is how long it would take to switch these systems. He also asked if companies could let state insurance regulators know how long it would take. Amann said the company would already have determined the data that is not needed before the 90-day period starts. Diederich said companies are requesting standards rather than prescriptive solutions, so companies need to let the Working Group know if they are following the National Institute of Standards and Technology (NIST), Insurance Services Office (ISO), or any other type of industry data standard.

© 2023 National Association of Insurance Commissioners

3. Discussed Other Matters

Johnson reminded attendees about the in-person interim Working Group meeting to be held in Kansas City, MO, June 5–6. She said the purpose of this meeting is to collaborate with state insurance regulators, consumer representatives, and industry members on revised wording for the most complex topics in the new draft of Model #674. Johnson thanked state insurance regulators, consumer representatives, and industry members who had submitted requests to be added to the registration invitation for this meeting, as the venue limits seating.

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

SharePoint/NAIC Support Staff Hub/Committees/H Cmte/WG-Privacy/050223 Call/Minutes_PPWG_050223.docx

Draft: 5/4/23

Privacy Protections (H) Working Group
Virtual Meeting
April 18, 2023

The Privacy Protections (H) Working Group of the Innovation, Cybersecurity, and Technology (H) Committee met April 18, 2023. The following Working Group members participated: Katie Johnson, Chair (VA); Cynthia Amann, Co-Vice Chair (MO); Chris Aufenthie, Co-Vice Chair (ND); Chelsy Maller (AK); Gio Espinosa and Catherine O'Neil (AZ); Damon Diederich (CA); C.J. Metcalf and Erica Weyhenmeyer (IL); LeAnn Crow (KS); Ron Kreiter (KY); Alexander Borkowski and Van Dorsey (MD); Jeff Hayden (MI); Santana Edison (ND); Teresa Green (OK); Gary Jones (PA); Patrick Smock (RI); and Todd Dixon (WA). Also participating was Doug Ommen (IA).

1. Discussed Private Right of Action (Section 28–Individual Remedies)

Johnson said the Working Group would be discussing the use of the following private right of action wording from the *Insurance Data Security Model Law* (#668) in place of the wording in Section 28(A) and (B) in the new *Insurance Consumer Privacy Protection Model Law* (#674):

> *This Act may not be construed to create or imply a private cause of action for violation of its provisions, nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this Act.*

Shelby Schoensee (American Property Casualty Insurance Association—APCIA) said the APCIA would be okay with the wording, as it is better than that in the original Feb. 1 exposure draft. Bob Ridgeway (America's Health Insurance Plans—AHIP) said he is okay with it, but he reserved the right to change his opinion in the future if necessary. Kristin Abbott (American Council of Life Insurers—ACLI) said she welcomes the change, particularly the removal of Part B. Chris Petersen (Arbor Strategies LLC), representing the Health Coalition, said legislators and state insurance regulators he had spoken with are against including a new private right of action, as the current version in Model #668 would maintain the status quo and not take away any protection from consumers.

Birny Birnbaum (Center for Economic Justice—CEJ) asked for the reason for this change. Johnson said it is because comments received were leaning strongly against the new wording, and no comments had been received leaning strongly in favor of the new wording. Birnbaum asked why the NAIC needs consumer representatives if state insurance regulators are going to do what industry members say. He said privacy differs from security, and the set of company actions differs. He said Model #668 is based on the federal Fair Credit Reporting Act (FCRA), which has a private cause of action, so Model #674 should have it. He posited that if a company takes data without the consumer's consent and the consumer's personal information is stolen, the consumer is harmed. He said a private cause of action would give the consumer an opportunity for redress. He also said this comment is in the comment letter submitted and signed by seven NAIC consumer representatives. Karrol Kitt (University of Texas at Austin) said she supports what Birnbaum is trying to say. She asked how else consumers would get redress. Peter Kochenburger (Southern University School of Law) said he supports what Birnbaum said, and industry never supports any private right of action. Michael DeLong (Consumer Federation of America—CFA) said he agrees with Birnbaum that not having a private right of action would hurt consumers, and it appears state insurance regulators are carrying water for industry. Bonnie Burns (Consultant to Consumer Groups) said she also supports Birnbaum's comments, and it appears that state insurance regulators and industry are on one side of this issue while consumer representatives are on the other side. Birnbaum said there is no evidence or reason for industry to oppose this except for the fact that state insurance regulators can enforce and protect consumers. Harry Ting (Consumer

Healthcare Advocate) said Europe has not been able to control this issue. Birnbaum said there is no status quo on consumers' data. He said we must have a surveillance economy now, and the consequences of losing data are great.

Smock said this change does not affect existing private right of action regulations. He said it depends on the jurisdiction as to whether it has or does not have a private right of action. The new wording allows each state to keep the private right of action or lack thereof that it currently has under law.

2. Discussed the HIPAA Safe Harbor

Johnson said the next topic to be discussed is the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Safe Harbor in Section 19 of Model #674. Petersen said the Health Coalition's comment letter noted that HIPAA preempts state law where it does not conflict and includes a safe harbor that will apply to all HIPAA-compliant companies. He said Model #674 should remove the words "subject to" and only use "compliant with," which is stronger wording. Johnson said Model #674 currently says, "subject to and compliant with." Ridgeway echoed what Petersen said because larger holding companies have health insurers and non-health insurers or companies, so HIPAA should apply to both. He also said the Working Group should want to adopt the most rigid structure regarding data privacy that it can. Birnbaum said the redline in question should say, "… if compliant with HIPAA; not subject to #674," and that it would give safe harbor. He also asked if states would go in to check on whether the companies are HIPAA-compliant. He asked that it be limited to companies that are subject to HIPAA. He also said this is the same as in the *Suitability in Annuity Transactions Model Regulation* (#275), which has caused lots of problems and tremendous confusion holding up even the frequently asked questions (FAQ) document explaining it. Johnson told Birnbaum what he meant by the phrase, "there is no agency to enforce it." Birnbaum said the wording, "subject to HIPAA" would require state and federal oversight of a company that is not subject to HIPAA.

Bradner asked what other lines are only subject to HIPAA, such as health services and property/casualty (P/C) companies compliant with HIPAA. He asked if other lines are subject to HIPAA or Model #674. Birnbaum asked if State Farm says it is compliant with HIPAA, whether states only look at HIPAA or state insurance regulators look at state insurance laws. Petersen said all personal information is protected the same as protected information. He said this is not new. It is in the federal Gramm-Leach-Bliley Act (GLBA) via the *Privacy of Consumer Financial and Health Information Regulation* (#672) and other state legislation via cybersecurity as "compliant with HIPAA." Ridgeway said the concern in California was that companies with HIPAA and non-HIPAA companies both used HIPAA for all lines to create administrative efficiencies, and he is trying to do the same for Model #674. He said an inquiry from the state would resolve any issues, which usually end up checking for clerical error. Aufenthie said it was unclear from the comments submitted by the Blue Cross Blue Shield Association (BCBSA) whether they agreed with the edits being suggested by Ridgeway during this call. Johnson said the comments submitted by the BCBSA referenced personal health information and not the broader term "all personal information," so it was unclear whether the BCBSA was suggesting the same edits as AHIP. She asked Randi Chapman (BCBSA) if she could shed some light on this question. Chapman said she needs to check with her policy person. Johnson asked Chapman to let Lois E. Alexander (NAIC) know if their policy references personal health information or the broader term "all personal information."

3. Discussed Other Matters

Johnson reminded attendees about the in-person interim Working Group meeting to be held in Kansas City, MO, on Monday, June 5, and Tuesday, June 6. She said the purpose of this meeting is to collaborate with state insurance regulators, consumer representatives, and industry members on revised wording for the most complex topics in the new draft of Model #674. Johnson thanked state insurance regulators, consumer representatives, and industry members who had submitted requests to be added to the registration invitation for this meeting, as the venue limits seating.

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

SharePoint/NAIC Support Staff Hub/Committees/H Cmte/WG-Privacy/Minutes_PPWG_041823_V2.docx

© 2023 National Association of Insurance Commissioners