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. Discussed Definitions of Insurance Transactions and Additional Permitted Transactions

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. Discussed the Contents Necessary to Have in a Notice of Consumer Privacy Practices

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/Committees/H Cmte_2023_Summer_WG-Privacy_Interim In Person PPWG Minutes_PPWG Interim Mtg_060523-060623

